Legal Risk Associated with Electronic Funds Transfer

by

SAMAHIR MOHAMMED ALI ABDULAH

A thesis submitted to Plymouth University

in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

Plymouth Law School

2014

Copyright Statement

I dedicate this work with all my love to my country

Iraq

for its unlimited benevolence and inspiration

Samahir

Legal Risk Associated with Electronic Funds Transfer

Samahir Mohammed Ali Abdulah

Abstract

The past thirty years have seen rapid advances in the technological component of banking services and as a consequence new legal issues have come to the fore, especially with regard to Electronic Fund Transfers (EFTs) which are now used to transfer money around the world, and have made fund transactions between payers and payees easier, faster and more secure. The method involves risks for both banks and customers, due to the possibility of unauthorized payments risks, credit and insolvency problems, and confidentiality issues. Most contracts and obligations now depend on the new technology, although there is a variety of methods for dealing with the concomitant risks. EFTs share a number of similarities with paper-based funds transfers in regard to methods of regulation, and the careful observer can identify patterns and themes.

Today, the business world depends heavily on EFT systems for its procedures; and government and academia have also taken a keen interest in EFTs. This thesis reviews and examines the existing legal position of liability of banks and customers for risks associated with EFT transactions: unauthorized EFT instruction and the problem of customer identity, credit risk and privacy, especially, the systems employed for safeguarding the customer's transactions and data. The thesis also makes recommendations for change.

The rules for the allocation of risk are based on the various mechanisms used to access the account. Also, due to the complexities of EFT, consumer protection becomes a paramount goal and is a subject of much concern, particularly when it comes to determining liability for losses. The UK government implemented the Payment Services Directive 2007 by adopting the Payment Services Regulations 2009, to regulate the system. However, such Regulations do not constitute a comprehensive regime that applies to all legal issues arising in the context of the EFT system. This study argues the necessity for a re-examination of existing laws and proposes a model for the future approach to the issues associated with EFT payment. Different approaches to EFT will be assessed, and the comparative and contrasting elements will be analysed in order to propose a comprehensive solution to the deficiencies in the current framework. Central to the problem is the absence of any uniform standard: individual banks offer differing contractual terms and conditions and different means of accessing accounts. Consequently it is time to formulate new and comprehensive rules for the allocation of liability of risks associated with EFT transactions.

Table of Contents

Dedication……ii
Abstract……iii
Table of Contents……v
List of Abbreviations……xi
Table of Cases……xiii
Table of Statutes……xxii
Table of UK Statutory Instruments……xxv
Table of Treaties and Conventions……xxvii
List of Tables and Figures……xxviii
Acknowledgements……xxx
Author's Declaration……xxxi

Chapter One……1
Introduction……1

1.1 The history and development of the clearing systems……4

1.2 Development of the EFT legal framework……7

1.2.1 The UNCITRAL Model Law on International Credit Transfers 1992……15

1.2.2 The Cross-Border Credit Transfers Directive 1997/5/EC……16

1.2.3 The Payment Services Directive 2007 (2007/64/EC)……20

1.2.4 The Payment Services Regulations 2009……21

1.3 Scope and objectives……23

1.4 Questions raised by the research……33

1.5 Methodology and structure of the thesis……34

Chapter Two……40
Legal aspects of EFT system……40

2.1 Introduction……40

2.2 Definition of EFT……41

2.3 EFT terminology……45

2.4 EFT systems categories……48

2.4.1 Credit and debit transfers……49

2.4.2 Non-customer-activated EFT systems……52

2.4.2.1 Clearance via BACS 52
2.4.2.2 Clearance via CHAPS 54
2.4.2.3 The Faster Payments Service 55
2.4.3 Consumer-activated EFT systems 57
2.4.3.1 Credit cards 58
2.4.3.2 Charge cards 60
2.4.3.3 Debit cards 61
2.4.3.4 ATM cards 64
2.4.3.5 Prepaid cards 65
2.5 The essential legal implications of EFT instructions 68
2.5.1 Sources of law 68
2.5.1.1 Law of agency 69
2.5.1.2 Law of contract 71
2.5.2 Plastic cards contractual schemes 72
2.5.2.1 Agreement between the card holder and the card issuer 73
2.5.2.2 Agreement between the merchant and the card issuer 73
2.5.2.3 Agreement between the merchant and the card holder 74
2.5.2.4 Agreement between the merchant and the merchant acquirer 75
2.5.3 The legal nature of the EFT instruction 76
2.5.3.1 An EFT instruction is not an assignment 77
2.5.3.2 An EFT instruction is not an negotiable instrument 79
2.5.3.3 An EFT instruction does not create trust funds 82
2.5.3.4 An EFT instruction constitutes a mandate 84
2.6 Conclusion 85

Chapter Three.....87
EFT parties' liability for unauthorized payment 87

3.1 Introduction 87

3.2 Unauthorized EFT instructions: identifying the problem 90

3.3 The basic schemes: authentication of EFT instructions 97

3.3.1 The existing law to authenticate EFT instruction and the problem of identity authorization.....98

3.3.2 Authentication procedures: functions, forms and validity 105

3.3.2.1. Electronic signature 111

3.3.2.2 The Trusted Third Party..... 115

3.3.2.3 The legal validity and recognition of electronic signatures as a signature 117

3.3.2.4 Liability of Certification Authorities and E-signatures.....123

3.4 EFT parties' liability for unauthorized transactions.....128

3.4.1 Customer's liability for unauthorized EFT transactions.....131

3.4.1.1 The duty of exercising care and skill not to facilitate fraud..... 136

3.4.1.2. Checking bank statements 142

3.4.2 The bank's liability for unauthorized EFT Transactions 149

3.4.2.1 Ambiguous EFT instructions 153

3.4.2.2 The bank's duty to prevent the facilitation of fraud 155

3.4.2.3 The bank's liability for its employees and agents 160

3.4.2.4 The bank's liability for adopting adequate security systems...167

3.4.2.5 Banking practice in guarding against unauthorized EFT transactions.....169

3.5 Conclusion 172

Chapter Four 174
EFT parties' liability for insolvency risk 174

4.1 Introduction 174

4.2 Execution of EFT instructions under the PSR 2009 176

4.2.1 Execution of EFT payment instructions 177

4.2.2 Execution time and value date of EFT transactions 181

4.2.3 Liability for non-execution of EFT transactions 184

4.3 Revocation and completion of EFT payment under common law rules 194

4.3.1 Identifying the problem 194

4.3.2 Revocation of EFT payment 196

4.3.3 Completion of EFT payment 198

4.3.3.1 EFT finality in transactions between bank accounts held in the same branch of the same bank (intra-branch) 203

4.3.3.2 EFT Finality in transactions between bank accounts held in different branches of the same bank (inter-branch) 212

4.3.3.3 EFT Finality in transactions between bank accounts held in a different banks (inter-bank) 213

4.4 The legal nature of payment devices 221

4.4.1. The conditional payment 221

4.4.2 The absolute payment 227

4.5 Allocating risk of EFT non-payment 230

4.6 Conclusion 236

Chapter Five 237
Privacy in the context of EFT 237

5.1 Introduction 237

5.2 The legal nature of confidentiality 239

5.3 Ambit, duration, and termination of the bank's a duty of confidentiality 242

5.4 Qualifications and exceptions to the duty of confidentiality 247

5.4.1 Disclosure by compulsion of law 247

5.4.1.1 Money launderingand the financing of terrorism.....254

5.4.1.2 Disclosure of confidential information to tax authorities.....258

5.4.1.3 Part XI of the FSMA 2000 260

5.4.2 Disclosure in the public interest 263

5.4.3 Disclosure in the bank's own interest.....265

5.4.4 Disclosure under the customer's authority 269

5.5 Disclosure of customer credit data to the Credit Reference Agencies (CRAs): legal issues 274

5.6 Analysis of the existing legal rules relating to the bank's duty of confidentiality in the EFT context.....282

5.6.1 The DPA 1998 and the protection of customers' electronic data 282

5.6.2 The Human Rights Act 1998 and misuse of customer's confidential information 286

5.6.3 The procedures actions against unauthorized access or any attack in the context of EFT 288

5.7 Liability for breach of the duty of confidentiality in an EFT context.....294

5.8 Conclusion 296

Chapter Six 299
Recoverability of EFT transaction losses 299

6.1 Introduction 299

6.2 The measure of damages for breach of contractual duty and its applicability to EFT transactions.....301

6.3 Damage category for recovery of EFT losses 303

6.3.1 Direct damage 304

6.3.2 Consequential damage 309

6.3.2.1 Recoverability of Currency Exchange Damages 312

6.3.2.2 The validity of the applicability of common law rules of consequential damages in EFT transactions.....317

6.4 Conclusion 320

Chapter Seven 322
Conclusion and proposals 322

7.1 The flaws of the PSR 2009 in the context of the allocation of risks associated with EFT 324

7.2 Allocation of unauthorized risk and the problem of identity authentication .. 326

7.3 Allocation of credit risk and the problem of EFT finality 330

7.4 Privacy and the problem of disclosure to CRAs 334

7.5 EFT, recoverability of damages and the problem of the validity of the applicability of common law rules of consequential damages 339

7.6 Recommendations 341

Bibliography 344

Books 344

Journal articles 353

Official documents and government publications 371

Media and Internet sources 372

Dissertations 373

Conference papers 374

List of Abbreviations

APACS	Association for Payment Clearing Services
ATM	Automated Teller Machine
BACS	Bankers' Automated Clearing Services
BEA	Bill of Exchange Act
CA	Certification Authority
C&CCC	Cheque and Credit Clearing Company
CCA	Consumer Credit Act
CHAPS	Clearing House Automated Payment System
CPAS	Cheque Printer Accreditation Scheme
CRA	Credit Reference Agency
DPA	Data Protection Act
FCA	Financial Conduct Authority
EC	European Community
ECHR	European Convention for the protection of Human rights and Fundamental Freedoms
EFT	Electronic Funds Transfer
EFTPOS	Electronic Funds Transfer at Point of Sale
EU	European Union
FSMA	Financial Services and Markets Act
LPA	Law of Property Act
OFT	Office of Fair Trading
PACE	Police and Criminal Evidence Act
PIN	Personal Identification Number
PSD	Payment Services Directive
PSR	Payment Services Regulations

SWIFT	Society for Worldwide Interbank Financial Telecommunication
TTP	Trusted Third Party
UCC	Uniform Commercial Code
ISDA	International Swaps and Derivatives Association
UKPA	UK Payment Administration
UNCITRAL	United Nations Commission on International Tread Law

Table of Cases

A v B Plc [2002] EWCA Civ 337; [2003] Q.B. 195

Afovos Shipping Co SA v R Pagnan & Fratelli (The Afovos) [1982] 1 W.L.R. 848

Agip (Africa) Ltd v Jackson [1991] Ch. 547

AIB Group (UK) Plc v Henelly Properties Ltd [2000] WL 1881366

Amstrad Plc v Seagate Technology Inc [1998] Masons C.L.R. Rep. 1

Arab Monetary Fund v Hashim (No.5) [1992] 2 All E.R. 911

Armagas Ltd v Mundogas SA (The Ocean Frost) [1986] A.C. 717

Arrow Transfer Co Ltd v Royal Bank of Canada [1972] R.C.S. 845

Ashworth Hospital Authority v MGN Ltd [2002] 1 W.L.R. 2033

Attorney-General v Guardian Newspapers Ltd (No. 2) [1990] 1 A.C. 109

Avraamides v Colwill [2006] EWCA Civ 1533

Awilco of Oslo A/S v Fulvia SpA di Navigazione of Cagliari (The Chikuma) [1981] 1 W.L.R 314

Balsamo v Medici [1984] 1 W.L.R. 951

Bank of England V Vagliano Bros. (1891) AC 107

Bank of Scotland v Alfred Truman [2005] EWHC 583 (QB)

Bank of Tokyo Ltd v Karoon [1987] A.C. 45

Bankers Trust Co v Shapira [1980] 1 W.L.R. 1274

Barclays Bank Ltd v WJ Simms Son & Cooke (Southern) Ltd [1980] Q.B. 677

Barclays Bank Plc v Quincecare Ltd [1992] 4 All E.R. 363

Barclays Bank Plc v Taylor [1989] 1 W.L.R. 1066

Basna v Punjab National Bank [1988] 2 All E.R. 296

Beswick v Beswick [1968] A.C. 58

Bhogal v Punjab National Bank [1988] 2 All E.R. 296

Boardman v Phipps [1967] 2 A.C. 46

Bolt and Nut Co (Tipton) Ltd v Rowlands Nicholls & Co Ltd [1964] 2 Q.B. 10

BP Plc v AON Ltd (No. 2) [2006] 1 C.L.C. 881

Brandeaux Advisers (UK) Ltd v Chadwick [2010] EWHC 3241 (QB)

Brewer v. Westminster Bank Ltd [1952] 2 All E.R. 650

British & Commonwealth Holdings plc (Joint Administrators) Respondents v Spicer & Oppenheim [1993] A.C. 426

Brown v Westminster Bank Ltd [1964] 2 Lloyds Report 187

BskyB Ltd v HP Enterprise Services UK Ltd [2010] EWHC 862 (TCC)

Bucknell v Bucknell [1969] 1 W.L.R. 1204

Calico Printers Association v Barclays Bank Ltd (1931) 39 Lloyd's List Rep. 51

Campbell v MGN [2004] 2 A.C. 457

Catlin v Cyprus Finance Corp (London) Ltd [1983] Q.B. 759

Charge Card Services Ltd (No.2), Re [1987] Ch.150; [1989] Ch. 497

Chatterton v London and Country Bank, The Times, 21 January 1891

Cinema Plus Ltd v ANZ Banking Group Ltd (2000) 35 ACSR 1

Commissioner of Police of the Metropolis v Charles (Derek Michael) [1977] A.C. 177

Common Services Agency v Scottish Information Commissioner [2008] 1 W.L.R. 1550

Coutts Co v Stock [2000] 1 W.L.R. 906

Crouch v Credit Foncier of England Ltd (1872-73) L.R. 8 Q.B. 374

Curran v Newpark Cinemas [1951] 1 All E.R. 295

Customs and Excise Commissioners v Barclays Bank Plc [2007] 1 A.C. 181

Customs and Excise Commissioners v FDR Ltd [2000] S.T.C. 672

Customs and Excise Commissioners v National Westminster Bank Plc (Authorisation: Mistake) [2002] EWHC 2204 (QB)

Customs and Excise v Diners Club Ltd [1989] 1 W.L.R. 1196

DB Deniz Nakliyati TAS v Yugopetrol [1992] 1 W.L.R. 437

Deposit Protection Board v Barclays Bank Plc [1994] 2 A.C. 367

Derby & Co Ltd v Weldon (No. 9) [1991] 1 W.L.R. 652

Derry v Peek (1889) 14 App. Cas. 337

Devonald v Rosser and Sons [1906] 2 K.B. 728

Di Ferdinando v Simon Smits and Co Ltd [1920] 3 K.B. 409

Do-Buy Limited v National Westminster Bank Plc [2010] EWHC 2862 (QB)

Dunlop Pneumatic Tyre Company Ltd v Selfridge and Company Ltd [1915] A.C. 847

Durant v Financial Services Authority [2004] F.S.R. 28

Durham Bros v Robertson [1898] 1 Q.B. 765

Easton v London Joint Stock Bank [1886] 34 Ch. D. 95

Eckmam v Midland Bank Ltd [1973] Q.B. 519

Empresa Cubana de Fletes v Lagonisi Shipping Co Ltd (The Georgios C) [1971] 1 Q.B. 488

Esso Petroleum Co Ltd v Milton [1997] 1 W.L.R. 938

European Asian Bank AG v Punjab & Sind Bank (No. 2) [1983] 1 W.L.R. 642

Eyles v Ellis (1827) 130 E.R. 710

Ezsias v Welsh Ministers [2007] All ER (D) 65 (Dec)

Fanmailuk.com Ltd v Cooper [2010] EWHC 2647 (Ch)

Fielding v Royal Bank of Scotland Plc [2004] WL 62144

Financial Institutions Services Ltd v Negril Negril Holdings Ltd [2004] UKPC 40

First Sport Ltd v Barclays Bank Plc [1993] 1 W.L.R. 1229

Firstpost Homes Ltd v Johnson [1995] 1 W.L.R. 1567

Fleming v Bank of New Zealand [1900] A.C. 577

Foley v Hill (1848) 9 E.R. 1002

Foskett v McKeown [2001] 1 A.C. 102

Garnett v M'Kewan (1872) LR 8 Ex

Genki Investments International Ltd v Ellis Stockbrokers Ltd [2008] 1 B.C.L.C. 662

George Mitchell (Chesterhall) Ltd v Finney Lock Seeds Ltd [1983] 2 A.C. 803

Gibson v Minet (1824) 130 E.R. 206

Good Challenger Navergante SA v Metalexportimport SA [2004] 1 Lloyd's Rep. 67.

Goodman v J Eban Ltd [1954] 1 Q.B. 550

Goodwin v News Group Newspapers Ltd [2011] E.M.L.R. 27

Goodwin v Robarts (1876) 1 App. Cas. 476

Governors of the Peabody Donation Fund v Sir Lindsay Parkinson & Co Ltd [1985] A.C. 210

Greenwood v Martins Bank Ltd [1933] A.C. 51

Grosvenor Casinos Ltd v National Bank of Abu Dhabi [2008] 1 C.L.C. 399

Hadley v Baxendale [1854] 9 Ex. 341

Halifax Union v Wheelwright (1874-75) L.R. Ex. 183

Hedley Byrne & Co Ltd v Heller & Partners Ltd [1964] A.C. 465

Heinl v Jyske Bank (Gibraltar) Ltd [1999] Lloyd's Rep. Bank. 511

Hely-Hutchinson v Brayhead Ltd [1968] 1 Q.B. 549

Henderson v Merrett Syndicates Ltd (No.1) [1995] 2 A.C. 145

Honourable Society of the Middle Temple v Lloyds Bank Plc [1999] C.L.C. 664

Horne v Midland Railway (1872-73) L.R. 8 C.P. 131

Howglen Ltd (Application for Disclosure), Re [2001] B.C.C. 245

Hughes v Pump House Hotel Co Ltd [1902] 2 K.B. 190

Imerman v Tchenguiz [2009] EWHC 2902 (QB)

Inner West London Assistant Deputy Coroner v Channel 4 Television Corporation [2008] 1 W.L.R. 945

International Minerals & Chemical Corp v Karl O Helm AG [1986] 1 Lloyd's Rep. 81

IR Commrs v Conbeer & Anor [1996] B.C.C. 189

Jackson v Royal Bank of Scotland [2005] 1 W.L.R. 377

Joachimson v Swiss Bank Corporation [1921] 3 K.B. 110

K Ltd v National Westminster Bank Plc [2007] 1 WLR 311

Kayford Ltd (In Liquidation), Re [1975] 1 W.L.R. 279

Keith Smeaton v Equifax Plc [2012] EWHC 2322 (QB); [2013] EWCA Civ 108

Kepitigalla Rubber Estates v National Bank of India Ltd [1909] 2 K.B. 1010

Koo Golden East Mongolia v Bank of Nova Scotia [2008] Q.B. 717

Laemthong International Lines Co Ltd v Artis (The Laemthong Glory) (No.2) [2005] 1 C.L.C. 739

Les Affreteurs Reunis v Walford [1919] A.C. 801

Libyan Arab Foreign Bank v Bankers Trust Co [1989] Q.B. 728

Libyan Arab Foreign Bank v Manufacturers Hanover Trust Co (No.2) [1989] 1Lloyd's Rep. 608

Linklaters v HSBC Bank Plc [2003] 2 C.L.C. 162

Lipkin Gorman v Karpnale Ltd [1989] 1 W.L.R. 1340

Lloyd v Grace, Smith & Co [1912] A.C. 716

Lloyds Bank Plc v Independent Insurance Co Ltd [2000] Q.B. 110

Lloyds Bank Plc v Voller [2000] 2 All E.R. (Comm) 978

London & County Banking Co Ltd v London & River Plate Bank Ltd (1887) 20 Q.B.D. 232

London CC v Agricultural Food Products [1955] 2 W.L.R. 925

London Intercontinental Trust v Barclays Bank [1980] 1 Lloyd's Rep. 241

London Joint Stock Bank Ltd v Macmillan [1918] A.C. 777

Lumley v Gye (1853) 118 E.R. 749

Mardorf Peach & Co Ltd v Attica Sea Carriers Corp of Liberia (The Laconia) [1976] Q.B. 835; [1977] A.C. 850

Messenger Newspapers Group v National Graphical Association (NGA) [1984] I.C.R. 345

Midland Bank Ltd v Seymour [1955] 2 Lloyds' Rep. 147

Minories Finance v Afribank Nigeria Ltd [1995] 1 Lloyds's Rep. 134

Mitsui & Co Ltd v Nexen Petroleum UK Ltd [2005] EWHC 625 (Ch)

Momm v Barclays Bank International Ltd [1977] Q.B. 790

Morison v London County and Westminster Bank Ltd [1914] 3 KB 356

National Bank of Commerce v National Westminster Bank Plc [1990] 2 Lloyd's Rep. 514

Newborne v Sensolid (Great Britain) Ltd [1954] 1 Q.B. 45

Niemietz v Germany (A/251-B) (1993) 16 E.H.R.R. 97

Norwich Pharmacal Co v Customs and Excise Commissioners [1974] 1 A.C. 133

Office of Fair Trading v Abbey National [2008] C.T.L.C. 1; [2010] 1 A.C. 696

Office of Fair Trading v Lloyds TSB Bank Plc [2006] 3 W.L.R. 452; [2008] A.C. 316

O'Rourke v Darbishire [1919] 1 Ch. 320

Orton v Collins [2007] 1 W.L.R. 2953

Overbrooke Estates Ltd v Glencombe Properties Ltd [1974] 1 W.L.R. 1335

Ozalid Group (Export) Ltd v African Continental Bank Ltd [1979] 2 Lloyd's Rep. 231

Parry-Jones v Law Society [1969] 1 Ch.1

Patel v Standard Chartered Bank [2001] Lloyd's Rep. Bank. 229

Paxton v Courtnay [1860] 175 E.R. 991

Pereira Fernandes SA v Mehta [2006] 1 W.L.R. 1543

Picker v London & County Banking Co Ltd (1887) 18 Q.B.D. 515

President of India v Lips Maritime Corp (The Lips) [1988] A.C. 395

Price Meats Ltd v Barclays Bank Plc [2000] 2 All E.R. (Comm) 346

Prudential Assurance Co Ltd v Ayres [2008] EWCA Civ 52; [2008] L. & T.R. 30

R. v Da Silva [2007] 1 WLR

R. v Dadson (1983) 77 Cr. App. R. 91

R. v Governor of Brixton Prison, Ex p. Levin [1997] Q.B. 65

R. v Hollinshead [1985] A.C. 975

R. v King (Hugo Allen) [1992] Q.B. 20

R. v Lambie [1982] A.C. 449

R. v Preddy [1996] A.C. 815

R. v Southwark Crown Court Ex p. Bowles [1998] Q.B. 243

R. v Special Commissioners of Income Tax [2002] 2 W.L.R 255

Regal Ltd v Gulliver [1967] 2 A.C. 134

Rekstin v Severo Sibirsko Gosudarstvennoe Akcionernoe Obschestvo Komseverputj [1933] 1 K.B. 47

Robertson v Canadian Imperial Bank of Commerce [1994] 1 W.L.R. 1493

Robinson v Harman (1848) 154 E.R. 363

Royal Products v Midland Bank [1981] 2 Lloyd's Rep. 194

Sale Continuation Ltd v Austin Taylor & Co Ltd [1968] 2 Q.B. 849

Schebsman (Deceased) Ex p. Official Receiver, Re [1944] Ch. 83

Scholey v Ramsbottom (1810) 170 E.R. 1227

Scott v Commissioner of Police of the Metropolis [1975] A.C. 819

Sempra Metals Ltd v Inland Revenue Commissioners [2008] 1 A.C. 561

Seven Seas Properties Ltd v Al-Essa (No.2) [1993] 1 W.L.R. 1083

Sewell v Corp (1824) 171 E.R. 1245

Shah v HSBC Private Bank (UK) Ltd [2009] EWHC 79 (QB); [2010] Bus. L.R. 1514; [2013] Bus. L.R. D38

Simpson v London & North Western Railway Co (1876) 1 Q.B.D. 274

Siqueira v Noronba [1934] A.C. 332

Smith v Lloyds TSB Bank Plc [2005] EWHC 246 (Ch)

Smith v Prosser [1907] 2 K.B. 735

Spectrum Plus Ltd (In Liquidation), Re [2005] 2 A.C. 680

Sphere Drake Insurance Ltd v Euro International Underwriting Ltd [2003] EWHC 1636 (Comm)

St Albans City and DC v International Computers Ltd [1997] F.S.R. 251

Standard Bank London Ltd v Bank of Tokyo Ltd [1995] C.L.C. 496

Strathlorne Steamship Co Ltd v Hugh Baird & Sons Ltd 1916 S.C. (H.L.) 134

Sunderland v Barclays Bank Limited (1938) 5 LDAB 163

Sutherland v Royal Bank of Scotland Plc [1997] S.L.T. 329

Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd [1986] A.C. 80

Tayeb v HSBC Bank Plc [2005] 1 C.L.C. 866

Tenax Steamship Co v Owners of the Motor Vessel Brimnes (The Brimnes) [1973] 1 W.L.R. 386; [1975] Q.B. 929

Torkington v Magee [1902] 2 K.B. 427

Tournier v National Provincial and Union Bank of England [1924] 1 K.B. 461

Transfield Shipping Inc v Mercator Shipping Inc (Achilleas) [2009] 1 A.C. 61

Trendtex Trading Corp v Credit Suisse [1982] A.C. 679

Tucker v Linger (1883) 8 App. Cas. 508

Turner v Royal Bank of Scotland Plc [2001] EWCA CIV 64

Van Lynn Developments Ltd v Pelias Construction Co [1969] 1 Q.B. 607

Victoria Laundry (Windsor) v Newman Industries [1949] 2 K.B. 528

Volkering v District Judge Haughton [2005] IEHC 240

Wai Yu-Tsang v R (1991) 1 WLR 1006

Warlow v Harrison (1859) 120 E.R. 920

Wealden Woodland (Kent Ltd v National Westminster Bank Ltd [1984] E.C.C. 203

Weld Blundell v Stephens [1920] A.C. 956

Wells v First National Commercial Bank [1998] P.N.L.R. 552

WF Harrison & Co v Burke [1956] 1 W.L.R. 419

Williams v Barclays Bank Plc [1988] Q.B. 161

Wilson v First County Trust Ltd (No 2) [2004] 1 A.C. 816

WJ Alan & Co Ltd v El Nasr Export & Import Co [1972] 2 Q.B. 189

Woods v Martins Bank [1958] 1 W.L.R. 1018

Young v Grote (1827) 130 E.R. 764

Table of Statutes

UK

Bankers' Books Evidence Act 1879

Banking Act 2009

Bills of Exchange Act 1882

Cheques Act 1957

Civil Evidence Act 1995

Competition Act 1998

Computer Misuse Act 1990

Consumer Credit Act 1974

Contracts (Rights of Third Parties) Act 1999

Criminal Justice Act 1987

Criminal Justice Act 1988

Criminal Law Act 1977

Data Protection Act 1998

Electronic Communications Act 2000

Extradition Act 1989

Financial Services and Markets Act 2000

Fraud Act 2006

Human Rights Act 1998

Income and Corporation Taxes Act 1988

Income Tax Act 2007

Insolvency Act 1986

Interpretation Act 1978

Law Commissions Act 1965

Law of Property Act 1925

Misrepresentation Act 1967

Police and Criminal Evidence Act 1984

Postal Services Act 2000

Proceeds of Crime Act 2002

Sale of Goods Act 1979

Statute of Frauds 1677

Supply of Goods and Services Act 1982

Taxes Management Act 1970

Terrorism Act 2000

Unfair Contract Terms Act 1977

EU Directives

Directive 1997/5/EC on cross-border credit transfers [1997] OJ L043/25

Directive 1998/26/EC on settlement finality in payment and securities settlement systems, amended by Directive 2009/44/EC OJ L146, and Directive 2010/78/EU OJ L331 [1998] OJ L166/45

Directive 1999/93/EC on a Community framework for electronic signatures [2000] OJ L13/12

Directive 2007/64/EC on payment services in the internal market amending Directives 1997/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 1997/5/EC [2007] OJ L319/1

Directive 2008/84/EC on credit agreement for consumers and repealing Council Directive 1987/102/EEC [2008] OJ L133/66

Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7

Directive 2011/83/EU on consumer rights, amending Directive 93/13/EEC and Directive 1999/44/EC and repealing Directive 85/577/EEC and Directive 97/7/EC [2011] OJ L304, 22/11

USA

Uniform Commercial Code

Table of UK Statutory Instruments

Civil Procedure Rules (SI 1998/3132) (L.17)

Consumer Credit (Disclosure of Information) Regulations 2010 (2010/1013)

Consumer Credit (Exempt Agreements) Order 1989 (SI 1989/869)

Consumer Credit Regulations 2010 (2010/1010)

Consumer Protection (Distance Selling) Regulations 2000 (SI 2000/2334), amended by Consumer Protection (Distance Selling) (Amendment) Regulations 2005 (SI 2005/689)

Cross-Border Credit Transfers Regulations1999 (SI 1999/1876)

Cross-Border Insolvency Regulations 2006 (SI 2006/1030)

Deregulation (Bills of Exchange) Order 1996 (SI 1996/2993)

Electronic money (Miscellaneous Amendments) Regulations 2002 (SI 2002/765)

Electronic Signatures Regulations 2002 (SI 2002/318)

Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (SI 1999/2979), amended by SI 2001/3929; SI 2002/1555; SI 2003/2096; SI 2006/50; SI 2006/3221; SI 2007/32; SI 2007/108; SI 2007/126; SI 2007/1655; SI 2009/1972 and SI 2010/2993

Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(SI 2001/544)

Money Laundering Regulations 2007 (SI 2007/2157) amended by Money Laundering (Amendment) Regulations 2007 (SI 2007/3299), by the Payment Services Regulations 2009 (SI 2009/209), The Money Laundering (Amendment No.2) Regulation 2011 (SI 2011/2833), and (SI 2012/2298)

Payment Services Regulations 2009 (SI 2009/209) amended by Payment Services (Amendment) Regulations 2009 (SI 2009/2475) and Payment Services Regulations 2012 (SI 2012/1791)

Unfair Terms in Consumer Contracts Regulations 1999 (SI 1999/2083)

Table of Treaties and Conventions

European Convention for the Protection of Human Rights and Fundamental Freedoms 1950

UNCITRAL Model Law on Electronic Signatures 2001

UNCITRAL Model Law on International Credit Transfers 1992

List of Tables and Figures

Tables

Chapter two

Table 1: Attributes and examples of cards payment ……... 67

Chapter three

Table 2: Customer's liability for unauthorized use of payment instrument under PSR 2009……. 135

Table 3: Banks' rights and obligations under Part 6 of the PSR 2009…….. 150

Chapter four

Table 4: Banks' Liability for non- execution payment instructions under Part 6 of the PSR 2009 ……. 192

Table 5: Comparison points between the PSR 2009 and Common law in the EFT finality……. 220

Figures

Chapter two

Figure 1: The Cross-Border Credit Transfer Regulations and UCC terminology……. 48

Figure 2: The PSR 2009 terminology……... 48

Figure 3: Credit transfer system…… 50

Figure 4: Debit transfer system……. 51

Figure 5: Funds movement through CHAPS Sterling system……. 55

Figure 6: The three party card schemes……. 75

Figure 7: The four party card schemes…… 76

Chapter Four

Figure 8: The Credit Card Schemes in *Re Charge Card Services Ltd*… 229

Acknowledgements

Not all that one knows is one's own. Most comes from hearing others or studying them. This thesis could not have been accomplished without the contribution of those who have preceded me in this field. To them I owe more than gratitude. I am extremely indebted in particular to my government, the Ministry of Higher Education and Scientific Research, Republic of Iraq, for believing in me and providing me with this scholarship and all the funding and support that has come with it.

Next, I would like to express my sincere thanks to the following people, without those kind support, advice and assistance this thesis would not have got off the ground successfully. Dr. Andrew Clark, my Director of Studies, was always there with clarifications when things got difficult or confused and his constructive suggestions during the planning and development of this research were of great value. His willingness to give his time so generously has been very much appreciated. Professor Peter Shears, my second supervisor, gave me time and logistical support whenever I needed it.

Finally, my heartfelt thanks go to my family, my parents who have given so much unconditional love and encouragement throughout my life, even in difficult moments, and my sisters and brother for their love which, without my family life would be meaningless.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

This study was financed with the aid of Ministry of higher education and scientific Research/Republic of Iraq. Relevant scientific seminars and conferences were attended at which work was presented and papers have been prepared for publication:

Publications

1- Abdulah, S., 'Electronic payment systems', (2012) 4 *Plymouth Law and Criminal Justice Review* 43-60.

2- Abdulah, S., 'The Bank's Duty of Confidentiality, Disclosure Versus Credit Reference Agencies; Further Steps for Consumer Protection: 'Approval Model', (2013) 19(4) *Web Journal of Current Legal Issues.*

Poster presentations

1- Abdulah, S., *The Payment Services Regulations 2009: is it a final solution to the legal issues arising in the context of Electronic Funds Transfer transactions?*, Postgraduate Law Conference, (May, 2012), University of London.

2- Abdulah, S., *An examination of aspects of liability for risks associated with Electronic Funds Transfer Transactions, with particular reference to*

the Payment Services Regulations 2009, The Postgraduate Society Annual Conference, (March, 2012), Plymouth University.

3- Abdulah, S., *Banks' liability in the Electronic Funds Transfer transactions risks*, The Postgraduate Society Annual Conference, (March, 2011), Plymouth University.

4- Abdulah, S., International Insolvency Law Conference, (September, 2010), Nottingham.

Oral presentations

1- Abdulah, S., *Defining Electronic Funds Transfers completion rules and allocating risk of non-payment: a 'proposal model'*, 8th Annual London Business Research Conference, (July, 2013), London.

2- Abdulah, S., *Electronic banking and identity authentication: risk allocation rules for authenticated but unauthorized payment*, International Conference on Business & Social Science, (June, 2013), Seoul.

3- Abdulah, S., *Electronic Funds Transfer and the problem of customer identity: Who should bear the risk*?, The Postgraduate Society Annual Conference, (June, 2013), Plymouth University.

4- Abdulah, S., *The legal nature of plastic cards payment*, Postgraduate Symposium, (May, 2011) Plymouth University.

Word count of main body of thesis: (81.311)

Signed……

Date:05/03/2014

Chapter One

Introduction

The world today is witnessing a tremendous development in the field of information technology, communication techniques, and rapid access to electronic data. The electronic revolution has changed the balance of economic and political forces. Thus, there is no way to disregard this new world influenced by science and technology, where information is not recorded on visible paper but transferred across an electronic screen. The world of information technology is thus a borderless world, which does not know geographical boundaries.

In line with this development, banks have created a new mode of funds transaction called “electronic banking” or “e-banking”.[1] In the context of the modern banking system via the Internet, ‘electronic banking’ is defined as ‘the provision of banking services and the issuing and performance of payments through the banking system by electronic means and other advanced technology’.[2] Thus, e-banking encompasses an entire set of processes through which a customer can transfer funds electronically without having to physically visit a bank, and these processes also include services where customers can access their accounts, conduct consumer and business transactions, receive

[1] The term 'banking' is framed in a particular way within the framework of English legislation, and is covered under the Banking Act 2009 and, the Financial Services and Markets Act 2000, Part 4, section 22, (FSMA 2000 hereafter).
[2] Gkoutzinis, A. A., *Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce* (2010), pp. 7-8.

necessary information on different financial services and products on the Internet.[3]

Thus, this form of banking has made transactions of funds between payers and payees easier and faster, which the services provided as outlined above are modified to meet contemporary needs: 24 hour account access; orders for payments; use of digital signatures; use of public access terminals such as the Automated Teller Machine (ATM) for making payments, internet shopping and direct electronic funds transfers.

The Electronic Funds Transfer or EFT constitutes one of the most significant banking services.[4] EFT is considered as the third of three significant generations in methods of payment.[5] The first generation method is cash, (notes and coins), while the second is bills of exchange and cheques.[6] The third, EFT, is a process by which, under instructions from a customer, a bank transfers funds from or to the customer's bank account by electronic means. EFT transactions occur within the existing UK framework of legal agreements, for example, agency law, contract law and the Payment Services Regulations 2009.[7] Regards to the EFT instruments like debit cards, credit cards or ATM cards, the agreement between the bank and the customer forms the legal

[3] Barclays, *Customer Agreement*, March 2012, http://www.barclays.co.uk/ImportantInformation/TermsandConditions/P1242575350746; HSBC, *General Terms and Conditions*, April 2012 http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf 9 January 2013.
[4] Dorn, J. A., *The future of Money in the Information Age* (1997), p. 23; UK Payments Administration, *Key Facts and Figures 2011*http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/ 22 February 2012.
[5] Arora, A, *Electronic Banking and the Law* (1988), p. 7.
[6] Frazer, P., *Plastic and Electronic Money: New Payment Systems and Their Implications* (1985), p. 3.
[7] Payment Services Regulations 2009 (SI 2009/209) amended by Payment Services (Amendment) Regulations 2009 (SI 2009/2475) and Payment Services Regulations 2012 (SI 2012/1791). (PSR 2009 hereafter).

contract between the two parties and shapes how any future dispute would be resolved.[8]

The system of funds transfer generally refers to the entire setup of a nation's financial institutions, like banks, and the associated practices that allow and facilitate the process of inter-bank fund transactions.[9] There are, however, several significant historical facts which must be understood because they shed considerable light on the issues involved in the development of EFT. The system of fund transfers was, until recently, primarily paper-based, normally through cash and cheques. It was only in 1960 that a shift in this traditional system of funds transfers occurred in the form of the EFT system.[10] The Post Office introduced the first national funds transfer operations. It granted the right to involvement in fund transfer facilities and was granted the right to supply full banking services to its customers. Two decades later, the bank fund transfer and the national fund transfer became connected, so that funds could be transferred from an account with a clearing bank to an account kept with the National Girobank.[11] Following this, in 1985, the National Girobank became a part of the clearing house. Subsequently it was acquired by Santander UK Plc. The Association for Payment Clearing Services was the only name used to describe the UK payments association, which existed to facilitate the cooperative activity of banks, building societies and card issuers.[12] However, in

[8] Kilonzo, K. D., 'An analysis of the legal challenges posed by electronic banking', (2007) 1 *Kenya Law Review* 323 at p. 325.
[9] UNCITRAL Legal Guide on Electronic Funds Transfers, United Nations (1987) http://www.uncitral.org/pdf/english/texts/payments/transfers/LG_E-fundstransfer-e.pdf 7 June 2011.
[10] The Post Office Act 1969, section 7(1)(b) which replaced by the Postal Services Act 2000, section 127(6) and Schedule 9.
[11] Giro notion is used to explain money transfer operations.
[12] Association for Payment Clearing Services (APACS hereafter).

July, 2009 the APACS replaced by the UK Payments Administration (UKPA), in favour of names that better described the different players in the payment system, since the UK payments industry has a number of different and separate clearing operations in industry groups.

1.1 The history and development of the clearing systems

Payment systems offer an account-based transfer service between two final customers. Transfers can occur between personal customers, between businesses or between personal and business customers.[13] The process of exchanging payment instructions between banks is called 'clearing'. In the UK there are four major clearing systems for giro transfers, responsibility for which is divided between four independent companies operating under the auspices of the UK Payments Council.[14] The reasons for involving different players in clearing operations systems are: firstly, there are different parts of the payment system; secondly, there are different numbers of parties involved in the clearing and settlement payment system. Finally, each party has functions and operations which are different from others. First, there is the credit clearing system run by the Cheque and Credit Clearing Company,[15] which is responsible for the clearing of paper-based credit transfer system, used for the physical exchange of high-volume and low-value transactions, for example, bank giro credit. C&CCC started in 1985, is a membership-based industry body with 11

[13] Office of Fair Trading, *UK payment systems: An OFT market study of clearing systems and review of plastic card networks,* 2003. http://www.oft.gov.uk/shared_oft/reports/financial_products/oft658.pdf 14 July 2013.
[14] UKPA, http://www.ukpayments.org.uk/ 14 July 2013.
[15] Cheque and Credit Clearing Company (C&CCC hereafter).

settlement members. In 2008 UKPA, decided to set a target date of 31 October 2018 for closing the central cheque clearing systems, with a final decision to be taken in 2016. Rahmatian believes that such a decision will not be of benefit to customers and is, therefore, against the replacement of the cheque as a payment method in the UK.[16] In contrast, Fisher argues that the cheque as a payment method has to end to protect customers from fraud.[17] Ellinger, et al. argue that the banking sector should consider investing the time and recourse into a sophisticated, fully-fledged system of cheque truncation. Finally, in 2011 the UKPA abandoned its decision and cheques will continue for as long as customers need them.[18]

Secondly, there is Bankers' Automated Clearing Services Limited,[19] which provides a high-volume, low-value, bulk electronic clearing service for credit and debit transfers, including direct debits and direct credits, where the payer sends his instructions directly to BACS rather than through a bank. BACS was established in 1968 and was considered the first clearing system relying on EFT. Until 1971 BACS was operated by the Inter-Bank Computer Bureau. Subsequently, BACS ran the system. In 1986, the company began to use the new name of BACS Limited. Later however, in 2004, BACS Limited was divided into BACS Payments Schemes Limited[20] and VocaLink.[21] In 2011, 5.6 billion

[16] Rahmatian, A., 'Must cheques disappear by 1018?', (2011) 26 *International Banking Law and Regulation* 310 at p. 311.
[17] Fisher, J., 'The UK's faster payment project: avoiding a bonanza for cybercrime fraudsters', (2008) 15 *Journal of Financial Crime* 155 at p. 162.
[18] Ellinger, et al., *Modern Banking Law* (2011), p. 397; Cox, R. and Taylor, J., 'Cheques', in Brindle, M. and Cox, R., *Law of Bank Payments* (2010), p. 497; UKPA, UK Payment Council, http://www.chequeandcredit.co.uk/cheque_and_credit_clearing/history_of_the_cheque/payment_dates_through_the_ages/-/page/2116/ 15 January 2013.
[19] Bankers' Automated Clearing Services Limited (BACS hereafter).
[20] BACS Payments Schemes Ltd is responsible for developing BACS services.

transactions have been made via BACS with a total value of £4.3 trillion.[22] The third clearing system is the Clearing House Automated Payment System,[23] a real-time gross settlement (RTGS) system, which is operated by the CHAPS Clearing Co Ltd.[24] CHAPS, provides a clearing service for international high-volume sterling credit transfers.[25] Finally, in May 2008 there is the CHAPS-operated 'Faster Payments Service', which provides a clearing service for high-volume, low-value sterling credit transfers, for example, internet and phone payments, which is based around the ATM and debit card messages, for less than £10,000 and standing orders for less than £100,000.[26] In November 2011, the responsibility for the Faster Payments Services was transferred from CHAPS to Faster Payments Scheme Limited.[27] Currently, there are ten member banks and building societies in the Faster Payments Scheme. By the end of 2011 over 85% of phone and internet payments were being processed through Faster Payments.[28]

The UK payment clearing systems described above have developed through the actions of commercial institutions and are not, in the main, the subjects of specific legislation or regulatory provisions. The most widely used clearings systems in value terms are owned and controlled by their members through the clearing companies under the UKPA umbrella.

---

[21] VocaLink runs the payment infrastructure which is now owned by 18 banks and building societies, see UKPA, http://www.ukpayments.org.uk/uk_payment_schemes/bacs/; Also, see http://www.vocalink.com 19 April 2013.
[22] UKPA, http://www.ukpayments.org.uk/uk_payment_schemes/bacs/ 19 April 2013.
[23] Clearing House Automated Payment System (CHAPS hereafter).
[24] UKPA, http://www.paymentscouncil.org.uk/who_do_we_work_with/payments_schemes/chaps/ 9 September 2013.
[25] *Ibid.*
[26] UKPA, http://www.ukpayments.org.uk/uk_payment_schemes/ 3 August 2012.
[27] UKPA, http://www.fasterpayments.org.uk/faster_payments/about_faster_payments/-/page/1941/ 9 September 2013.
[28] UKPA, http://www.fasterpayments.org.uk/faster_payments/about_faster_payments/-/page/1941/ 19 April 2013.

1.2 Development of the EFT legal framework

The development of transactions and funds transfers via the Internet, combined with the development of international commerce, needs predictable and clear rules under which customers' transactions occur. Customers are naturally adverse to the uncertainty and unpredictability inherent in the rules of law. They want certainty about the legal rules under which their transactions occur, since in this way customers can precisely measure and reduce the risks arising from EFT transactions. Regularity in the law across jurisdictions assists and helps to allocate and determine legal issues relating to EFT.[29] The payment system law in the UK is influenced by the European Union's programme, as the UK is a member of the EU, which was intended to create a single market in payment services by optimising efficiency, enhancing competition and innovation, increasing consumer choice and raising the standards of consumer protection across Europe.[30]

Since its creation, the European Union (EU) has been working diligently to establish optimal regulation at EU level,[31] although it is difficult to do so, because EU Member States traditionally seek to maintain a maximum space of national sovereignty. Through ongoing geographical enlargement and gradual European integration, the ideal of EU uniformity of laws lost some ground, as

[29] Bollen, R., 'Harmonisation of international payment law: a survey of the UNCITRAL model law on credit transfers: Part 1', (2008) 23 *International Banking Law and Regulation* 44 at p. 44.
[30] Brandt, P. and Graham, P., 'An update on the UK's implementation of the Payment Services Directive', (2009) 64 *Compliance Officer Bulletin* 1 at p. 2.
[31] Further, see Bollen, R., 'European regulation of payment services – the story so far', (2007) 22 *International Banking Law and Regulation* 451 at p. 452.

new claims for differentiation and flexibility made their appearance.[32] Likewise, the completion of the internal market required a reform of the legislative process to facilitate and accelerate the adoption of the necessary measures for its completion, since the existing techniques were slow and engendered excessive uniformity.[33]

"Harmonization" can be thought of as the process through which domestic laws may be modified to enhance predictability in cross-border commercial transactions, whereas "unification" is the adoption by States of common legal standard governing particular aspects of domestic and international business transactions.[34] Thus, it is important to investigate the harmonization of the EFT system in the European Union and look at its application in these areas. The reference to the new legal framework indicates that there are already in force legal instruments to regulate EFTs. Different legal frameworks have different legal effects. The relevant legal instruments are the Cross-Border Credit Transfers Directive 1997/5 and the Payment Services Directive 2007 (2007/64/EC).[35]

The transfer of funds between the payer's account and the payee's account when both have an account in the same branch of the same bank (an intra-branch transfer),[36] or at different branches of same bank (an inter-branch transfer), will require an adjustment of the balances of the payer's and payee's

[32] Mavromati, D., *The Law of Payment Services in the EU* (2007), p.85.
[33] *Ibid.*
[34] UNCITRAL website, *What does UNCITRAL mean by the "harmonization" and "unification" of the law of international trade?* http://www.uncitral.org/uncitral/en/about/origin_faq.html#harmonization 15 July 2013.
[35] European Payment Council, *SEPA Legal and Regulatory Framework* http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_legal_and_regulatory_framework 15 July 2013.
[36] *Libyan Arab Foreign Bank v Bankers Trust Co* [1989] Q.B. 728 at pp. 750-751.

accounts at that bank. The payer's account is debited and the payee's account is credited. In these circumstances, there is no transfer of funds between banks.

However, in most cases, the transfer of funds takes place in circumstances where the payer's account and the payee's account are held at different banks (inter-bank transfer). In an inter-bank transfer a payment instruction will transmit either directly from the payer's bank to the payee's bank or through intermediary banks to the payee's bank.[37] In these circumstances, there is therefore a transfer of funds between banks. This process is known as settlement and can occur on either a bilateral or multilateral basis.[38] Bilateral settlement takes place where both payer's and payee's banks have an account with the other. Settlement is effective through an adjustment of these accounts.[39] In contrast, multilateral settlement involves the settlement of accounts of the payer's bank and the payee's bank held at a third bank. The third bank could be a common correspondent of the both banks (payer's bank and payee's bank), where they both have accounts. Alternatively, the third bank could be a central bank. [40]

Settlement may be either gross or net. With gross settlement, the payer's bank and the payee's bank settle each payment instruction independently regardless of any other payment obligations issuing between the payer's bank and the payee's bank. In contrast, with net settlement, the reciprocal payment obligations of the payer's bank and the payee's bank are set off against each

[37] Mengle, D., *The Importance of Close-Out Netting*, (2010, ISDA Research Notes), p. 2.
[38] Ellinger, et al., *op.cit.,* p. 564; Cox, R. and Taylor, J., 'Fund Transfers', in Brindle, M. and Cox, R., *Law of Bank Payments* (2010), p. 60.
[39] Hapgood, M., et al., *Paget's Law of Banking* (2007), pp. 363-364.
[40] *Ibid.,* at p. 364; Ellinger, et al., *op.cit.,* p.564; Cox, R. and Taylor, J., 'Fund Transfers', *op.cit.,* p.60.

other and only the net balance paid.[41] In bilateral netting, a parties' position is measured by reference to its net position with regard to each separate counterparty, and not by reference to the settlement as a whole. In contrast, in multilateral netting, a parties' position is measured by reference to its net position with regard to all other parties in the settlement as a whole. Consequently, each party will end up as a net net-debtor or a net net-creditor in connection to all other parties in the settlement.[42] The legal ground for "netting" in the context of inter-bank settlements is based in contract. This is where the ISDA "master agreements" come into play.[43] "Master agreements" is the standardized, pre-printed form agreement published by the International Swaps and Derivatives Association (ISDA), which is used to document over the-counter (OTC) derivatives trades. The parties add to or modify the terms of the ISDA Master through the use of a Schedule to the ISDA master agreement. The ISDA Master, along with the Schedule to the ISDA Master Agreement, if any, are umbrella documents that parties typically use to govern their trading relationship, often covering many transactions (each of which is evidenced by a transaction confirmation) of different types.[44]

Netting settlement has an important advantage in that it reduces the quantity and value of settlement between accounts held at different banks, which helps to reduce transaction charges and improved liquidity. Furthermore, net settlement has advantages in relation to exposure to receiver risk. Normally in EFT, when a bank receives a payment instruction from another bank involved in

[41] Ellinger, et al., *op.cit.,* p.564.
[42] *Ibid.,* at pp. 564-565.
[43] http://www2.isda.org/about-isda/ 04 December 2013.
[44] *Ibid.*

a chain payment, the bank makes the transaction funds available to its customer before it has actually received the credit due on finalisation of the multilateral netting at the end of the day. Therefore, the collecting bank bears the risk that it may not be placed in funds. Moreover, when the bank acted on its customer's instruction, the receiving bank may itself pass on a payment order down a chain of banks. The default of one bank involved in the fund transfer to execute payment means that the other banks involved in the payment transaction have no ability to execute their own payment obligations.[45] This is called a systemic or credit risk.

In order to reduce systemic risk in payment systems that operate on the basis of payment netting, and to minimize the disruption caused by insolvency proceedings against a participant in a payment or securities settlement systems, the EC adopted Directive 98/26/EC on settlement finality in payment and securities settlement systems.[46] Article 3(1)[47] of the Directive provides that transfer instruction and netting are to be validly enforceable and binding on third parties, even in the result of insolvency proceedings, as long as the instructions for the transfer are entered into the system prior to the moment when the insolvency is deemed to have begun; article 3(2) provides against the "unwinding" of payment netting as a consequence of any national legislation or financial practices which allow transactions and contracts to be revoked in cases where they were concluded before the moment when the insolvency

[45] Hapgood, et al., *op.cit.,* p. 364.
[46] Directive 1998 on settlement finality in payment and securities settlement systems (1998/26/EC) OJ L166/45, amended by Directive 2009 (2009/44/EC) OJ l146, and Directive 2010 (2010/78/EU) OJ L331.
[47] Amended by article 1(6) of the Directive 2009 (2009/44/EC) OJ l146.

proceedings were initiated; article 5[48] decrees that there is to be no revocation of a transfer order on the part of a participant in the system or a third party from the moment which is defined in the rules; article 6(1) rules that the moment when the insolvency process begins is that when the judicial or administrative authority concerned announces its decision; [49] and finally, article 7[50] ensures that the insolvency proceedings do not retrospectively affect the obligations and rights of the participants as a consequence of the latter's participation in a system at a point earlier than the beginning of the proceedings. The UK has implemented the Directive of 1998 through the Financial Markets and Insolvency (Settlement Finality) Regulations 1999. [51] The Regulations 1999 apply only to systems that are accorded designation by a 'designating authority'.[52] In this capacity as a designating authority, the Bank of England granted the CHAPS Sterling clearing 'designated system' status.[53]

The legal framework of the European Union (EU) has developed differently and that has led to the development of a UK legal framework which is part from the EU, but which nevertheless does not respond directly to the risks associated with EFT. For example, the Directive of 1998 on settlement finality in payment and securities settlement systems provides insolvency proceedings but did not address the point at which the EFT transactions are to be considered final

[48] Amended by article 1(8) of the Directive 2009 (2009/44/EC).
[49] Further, see Sealy, L. S., 'The Settlement Finality Directive – points in issue', (2000) 2 *Company Financial and Insolvency Law Review* 221 at pp. 221-228.
[50] Amended by article 1(9) of the Directive 2009 (2009/44/EC).
[51] Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (SI 1999/2979), amendment by SI 2001/3929; SI 2002/1555; SI 2003/2096; SI 2006/50; SI 2006/3221; SI 2007/32; SI 2007/108; SI 2007/126; SI 2007/1655; SI 2009/1972 and SI 2010/2993.
[52] Regulations 3-12, Schedule 1 of the Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (as amended).
[53] Bank for International Settlements, Payment systems in the United Kingdom, in *The Red Book* (2003), p. 399 http://www.bis.org/publ/cpss53p14uk.pdf 17 July 2013.

between the banks, or between the banks and customers or between the payees and the payers. Also, it does not address the question of which party bears the risk of the insolvency of one of the banks involved in the EFT transactions. PSD 2007 does indeed address the rights, obligations and liabilities of both banks and customers in cases of unauthorized payment and non-execution or defective execution of a payment instruction where the payment is within the EU. However, it fails to address and solve the problem of customer identity, the finality of payment, intermediary bank's liability and customer's privacy. Therefore, there is a need to regulate the EFT system.

The lack of regulation of issues associated with EFT is a problem, as the existing rules applicable to EFT are insufficient to address the transactions' parties' rights, obligations and liabilities, which is costly to all concerned and discourages the use of the system. [54] The existing laws lack a consistent conceptual foundation and fail to address the problems of access to banking services, such as customer identity. The inadequacy of customer identification in the regulation of EFT payment, particularly payments by cards entails risks for consumer privacy. EFT regulation should require consumer protection in the use payment by card associations such as Visa and MasterCard, not only to make their rules public but also to regulate consumer protection, [55] for example, card issuer's right to chargeback facility.[56] Finally, EFT regulation should require consumer protection in relation to unfair terms in banker-customer contracts.

[54] Bollen supports such a view and argues that harmonisation reduces the risk that a problem will be treated and solved differently in other counties; Bollen, harmonisation of international payment law: a survey of the UNCITRAL model law on credit transfers: part 1, *op.cit.,* at pp. 44-45.
[55] Credit cards payment are protecting by Consumer Credit Act 1974.
[56] Rosenberg, A. S., 'Better than cash? global proliferation of payment cards and consumer protection policy', (2006) 60 *Consumer Finance Law Quarterly Report* 426 at p. 459.

Law is frequently created to give direction to new developments and to accomplish some political or social objective such as consumer protection.[57] Indeed, the goal of regulating EFT systems is not to obstruct progress but to protect the weaker party and prohibit abusive or unsound practices.[58] This thesis demonstrates that there is a need to regulate the EFT system and it seeks to vary the balance in the banker-customer relationship in favour of the customer.[59] Moreover, the EFT regulatory framework should distinguish between different types of customers, for example, businesses and consumers. Joris and Gutwirth[60] support the view that EFT system should be regulated under one body of law, for the following reasons: first, financially speaking, banks occupy an advantageous position, in that they can apply pressure to their customers with a view to gaining favourable conditions in bank-customer contracts. Secondly, it is essential that any steps which are taken for the protection of consumers should have a compulsory element.[61] Thirdly, regarding regulation of the most sensitive areas of EFT, such as encryption security, issues of liability and the burden of proof, guidelines which are entirely voluntary are clearly inadequate and unacceptable. Finally, it is a fact that payment instruments for example, cheque[62] and bill of exchange[63] have been

[57] Joris, T., and Gutwirth, S., 'Electronic Funds Transfer and the consumer: the "soft law" approach in the European Community and Australia', (1991) 40 (2) *International & Comparative Law Quarterly* 265 at p. 295.
[58] *Ibid.*
[59] *Report by the Review Committee on Banking Services: Law and Practice*, ("The Jack Report") (1989, London, HMSO, Cm 622), Ch. 10.
[60] Joris and Gutwirth, *op.cit*. p. 301.
[61] *Ibid.*
[62] Cheques Act 1957.
[63] Bills of Exchange Act 1882.

regulated by uniform legislation, although EFTs still operate satisfactorily, thus there is no reason to deal with such system in a different way.[64]

1.2.1 The UNCITRAL Model Law on International Credit Transfers 1992

The first approach that was adopted in 1992 by the United Nations Commission on International Trade Law was a Model Law on International Credit Transfers which dealt with cross-border credit transfers only.[65] The UNCITRAL Model Law was designed to address two significant changes in how fund transfers were handled internationally.[66] The first change was a promotion using electronic payment, and the second change was the general movement from debit transfers to credit transfers.[67] A credit transfer instruction is initiated by the payer who orders his bank to move funds from his account to the payee's bank account.[68] Thus, the payer's bank moves the amount of the transaction to the payee's bank by some form of credit transfer, such as a standing order. Conversely, a debit transfer instruction is initiated by the payee who orders his bank to request the funds from the payer's bank account, for example as a

[64] It is worth to clarify that the Department for Business, Innovation and Skills on 12 June 2013 published a draft Consumer Rights Bill which implemented the Consumer Rights Directive 2011/83/EU. The policy of Consumer Rights Bill is providing better information and protection for consumers: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206367/bis-19-925-draft-consumer-rights-bill.pdf, and the explanatory notates related to the Consumer Rights Bill https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206561/bis-13-926-draft-consumer-rights-bill-explanatory-notes.pdf 03 September 2013.
[65] United Nations Commission on International Tread Law (UNCITRAL hereafter), UNCITRAL website http://www.uncitral.org/uncitral/en/index.html 15 July 2013.
[66] Explanatory Note by the UNCITRAL Secretariat on the Model Law on International Credit Transfers, note 1.
[67] Dole, R. F., 'Receiving bank liability for errors in wholesale wire transfers', (1995) 69 *Tulane Law Review* 877 at p. 912.
[68] Cox, R. and Taylor, J., 'Funds Transfers', *op.cit.,* p. 57.

direct debit. The UNCITRAL Model Law attempted to regulate the essential rules, leaving the national authorities the freedom to regulate their own legal systems.

The creation of the single market in the EU after 1992 brought about an improved community regime for the business sector. The Commission, which had previously issued the Cross-Border Credit Transfers Directive, issued a Green Paper on the working of the payment system in the internal market. The Green Paper established the main principles of the payment systems under the single market.

The recommendations explained the area of cross-border credit transfers, but there was no organized application, which reduced the number of applications. This drove the Commission to issue a Communication on the transfer of funds. Subsequently, in 1997, the EU adopted the UNCITRAL Model Law on International Credit Transfers by implementing the Cross-Border Credit Transfers Directive.[69] This is the legal background which led to the issuing of the Cross-Border Credit Transfers Directive 1997/5.

1.2.2 The Cross-Border Credit Transfers Directive 1997/5/EC

Directive 1997/5/EC was the first legislative regime to deal explicitly with cross-border credit transfers at the EU level. The Directive covered retail credit transfers up to the value 50,000 Euros. The aim of EU innovations in this area was to facilitate intra-Community business by enabling international payments

[69] Cross-Border Credit Transfers Directive 1997/5/EC.

to become easy and effective as local payment.[70] The UK government implemented the 1997/5/EC Directive by establishing the Cross-Border Credit Transfer Regulations 1999,[71] which clarifies the responsibilities of institutions participating in the sending, processing and receipt of cross-border credit transfers. The central provisions of the Directive 1997/5 were as follows:

(a) Article 3 explained the conditions and requirements of the credit institutions and instructed customers how to make a cross-border credit transfer. It also provided information, for example, on the time needed for carrying out a credit transfer.

(b) Article 6 determined the time for the carrying out of a transaction, which was five days.

(c) Article 7 imposed several obligations on the banks, such as the obligation to transfer the full credit transaction's funds to the payee, and the obligation not to deduct any fund from the transaction's fund unless there was approval from the payer for such deductions.

(d) Article 8 established the rules of reimbursement in the case of the non-execution of the credit transfer by the bank. The 1997 Cross-Border Credit Transfers Directive came without any indication of the banks' rights to cancel credit transfers in accordance with the customer's request. Therefore, the European Economic Community member states have the right to issue or to retain their appropriate provisions on the matter.[72]

(e) Article 10 explained the rules of disputes between banks and customers relating to the payment settlement.

[70] Bollen, European regulation of payment services – the story so far, *op. cit.*, p. 462.
[71] Cross-Border Credit Transfer Regulations 1999 (SI 1999/1876).
[72] Mavromati, *op.cit.*, p. 70.

In comparing the UNCITRAL Model Law and the Directive 1997/5, it seems that the Directive 1997/5 placed more attention on protecting consumers than the UNCITRAL Model Law, (articles 3 and 7 of the Directive). Also there is a difference in the ambit of the application. The UNCITRAL Model Law was considered more comprehensive in that it covered all international transfers.[73] In contrast, the 1997/5 Directive covered only international transfers in the EU area and was limited to 50,000 Euros.[74] Another dissimilarity was that the UNCITRAL Model Law did not cover the time of execution of a conditional payment instruction,[75] whilst the Directive 1997/5 covered the time of execution both conditional and unconditional payment instruction t.[76]

As mentioned earlier, the aim of the 1997/5 Directive was to remove the obstacles of cross-border credit transfers within the EU Member States. The main focus is to facilitate transfer of funds easily and effectively as local payment. Some of these aims have been recognised but only to a limited extent.[77] However, many more legal and regulatory obstacles still impede the development of a dynamic and efficient payment system such as uniform rate for cross-border credit transfers in the single market.[78] Seyad argues that the most significant shortcoming in the 1997/5 Directive is that the Directive

[73] Bojer, L., 'International credit transfers, the proposed EC Directive compared with the UNCITRAL Model Law', (1995) 10 *International Banking Law* 223 at p. 224.
[74] Article 1 of the Cross-Border Credit Transfers Directive 1997.
[75] UNCITRAL Model Law, article 3.
[76] Directive 1997/5, article 11(1).
[77] Seyad, S. M., 'A critical assessment of the Payment Service Directive', (2008) 23 *International Banking Law and Regulation* 218 at p. 220.
[78] *Ibid.*

objectives are not adequately reflected in the measures employed nationally.[79] He believes that the 1997/5 Directive failed to achieve its aims.[80] He states:

> "The Member States have failed to sufficiently transpose the transparency requirements into their respective legal system. The nature and scope of information provided before and after the execution of cross-border credit transfers do not properly correspond to the requirements of the relevant legal instruments……. also failed to ensure a uniform rate for cross-border credit transfers in the single market."[81]

Indeed, the 1997/5 Directive failed to ensure a uniform rate for cross-border credit transfers in the EU. That is because the payment agents apply different charges for cross-border credit transfers based on country or destination, even though it is addressed within the EU. The charges may also differ depending on the currency denominated for a cross-border credit transfer.[82]

Eventually, a safe and efficient payment system should be modernised to reduce risks and increase trustworthiness and efficiency. Development of the electronic payment system in the EU made the Commission of the European Communities look for a Single Euro Payments Market to make the card payments and credit transfers easier, cheaper and safer. Central to the growth of the Single Euro Payment Market is the Payment Services Directive,[83] which should be viewed in the light of the achievement of these overall aims.

[79] *Ibid*
[80] *Ibid*
[81] *Ibid*
[82] Mavromati, *op.cit.*, pp. 68-69; Seyad, *op.cit*., p. 220.
[83] Payment Services Directive (2007/64/EC) O.J. (L 319/1). amends to directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC. Replaced Directive 97/5/EC. (PSD hereafter).

1.2.3 The Payment Services Directive 2007 (2007/64/EC)

The Cross-Border Credit Transfers Directive, 1997/5/EC, was replaced by the Payment Services Directive 2007 (2007/64/EC). The PSD 2007 aimed to harmonize the common legal framework and it intended to create a Single Euro Payments Market focussing on electronic payments.[84] The PSD 2007 also aims to promote the integration and rationalization of national payment systems and their underpinning national legislation.[85] The PSD 2007 was considered broader than Directive 1997/5 because it covered both Euro payments and Sterling payments to and from the UK. In brief, the essential goals of the PSD 2007 were improved economies of scale, thus generating more competition to help introduce a fair payment market system; also to present legally harmonized rules involving information requirements and the obligations and rights related to the banks and customers, with a consumer protection focus.[86]

Directive 2007 established a set of requirements for both banks and customers which must respect standard covering rules, these are: execution time - Directive 2007 sets a mandatory execution time of Day +1 for all credit transfers without any currency conversion; liability for non-execution or defective execution of a payment order where the payment is within the Member States; customer's liability for misuse of a payment instrument up to the value of 150

[84] European Payment Council, *SEPA Legal and Regulatory Framework* http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_legal_and_regulatory_framework 15 July 2013.
[85] Brandt and Graham, *op.cit.,* p. 2.
[86] Robertson, P., et al*.,* 'Internet Payments' in Brindle, M., et al*., Law of Bank Payments* (2010), p. 314; Bollen, R., 'European regulation of payment services – recent developments and proposed Payment Services Directive – Part 2', (2007) 22 *International Banking Law and Regulation* 532 at p. 539.

euros; and the full amount of the transaction must be credited in the payee's account and, any charges or fees must be recouped separately. The PSD 2007 applied to both retail and wholesale transactions. Furthermore, the PSD 2007 covered both debit and credit transfers. It applies whenever one or both transactions' parties are in the Member States. However, cheques and cash were outside the scope of Directive 2007. The reason for the exclusion is that those services cannot be processed efficiently as electronic payment.

The PSD 2007 had to be implemented into EU Member States' law by 1 November 2009. The UK was committed to meeting that deadline. In the UK, the Payment Services Regulations 2009 replaced the PSD 2007. The Payment Services Regulations 2009 have been made after extensive consultation both on the draft Directive 2007 and on the draft Regulations 2009 themselves.[87] The Payment Services Regulations 2009 were published on 9 February 2009.

1.2.4 The Payment Services Regulations 2009[88]

The PSR 2009 present a novel authorization regime, and allots rights to customers subject to information, for example, irrevocability of payment instructions, charges, and execution time. Generally, the PSR 2009 embraces all methods of electronic payment. It has a wide application to EFT transactions such as BACS, CHAPS, and payment by cards. Nevertheless, payment in cash and cheques are outside the scope of the Regulations 2009. PSR 2009 applies

[87] Brandt and Graham, *op.cit.,* p. 3.
[88] PSR 2009 (SI 2009/209); amended by Payment Services (Amendment) Regulations 2009 (SI 2009/2475), and Payment Services Regulations 2012 (SI 2012/1791).

to banker-customer transactions in the UK.[89] It also covers transactions between the payer's bank and the payee's bank within the European Economic Area.[90] The PSR 2009 embraces Sterling, Euro, and other European currencies,[91] although it executes transactions involving non-European currencies such as the American dollar.

The rights, duties and liabilities of the banker-customer relationship in the EFT are currently covered by the PSR 2009 when applicable. In this regard, the contractual rights, duties and liabilities will be determined according to Parts 5 and 6 of the PSR 2009. It introduces rights and obligations in respect of subjects' countermand of payment instructions, charges, execution time, internet payment via telephone or card, and the regulation of information.[92] However, PSR 2009 contain different rules for different types of customer, namely, "consumers",[93] businesses, "micro-enterprises"[94] and "charities".[95] Accordingly, the parties may agree to not apply regulations 60, 62, 63, 64, 67, 75, 76 and 77, where the customer is not a consumer, micro-enterprise or a charity.[96] The PSR 2009 have stipulated various information requirements from customers in framework contracts.[97] Information is requested at various times; it

[89] PSR 2009, regulations 33(1)(a) and 51(1)(a).
[90] *Ibid.,* regulations 33(1)(b) and 51(1)(b).
[91] *Ibid*., regulations 33(1)(c) and 51(1)(c).
[92] *Ibid.*, Parts 6.
[93] According to the regulation 2(1) of the PSR 2009 "consumer" means 'an individual who, in contracts for payment services to which these Regulations apply, is acting for purpose other than a trade, business or profession'.
[94] Regulation 2(1) of the PSR 2009 defines "micro-enterprise" as 'an enterprise which, at the time at which the contract for payment services is entered into, is an enterprise as defined in Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC(**c**)'.
[95] According to the regulation 2(1) of the PSR 2009 "charity" means 'a body whose annual income is less than £1 million and is (c) in England and Wales, a charity as defined by section 1(1) of the Charities Act 2006(**c**).'
[96] PSR 2009, regulations 51(3)(a).
[97] *Ibid.*, regulations 36-50.

is required before the payment order is passed;[98] after receipt of the payment order; [99] and after the payment order is carried out and the transaction executed.[100] Furthermore, there are information requirements for the bank when framework contracts are involved.[101]

These regulations, however, are not without flaws and deficiencies. Consequently, any EFT issues which are beyond the ambit of the regulations will be determined by the principles of common law, which deals with the duties and liabilities imposed by the banker-customer relationship and provide such remedy as may be necessary.

1.3 Scope and objectives

It is becoming increasingly difficult to ignore the EFT as a sophisticated method of payment, thus equally sophisticated consumer protection becomes a major goal and the question of liability for risks arising from using EFT is of great concern. Banking by its very nature is a high risk business. The major risks associated with EFT are unauthorized EFT payment, credit risk and privacy. The risk allocation rules existing on the basis of various mechanisms used to access the account and they do not provide realistic incentives for either the customer or the bank to safeguard against risks in a reasonable manner. There is no standard formula in the EFT system, which makes it difficult to identify which party bears the losses for unauthorized risk, non-payment or to determine

[98] *Ibid.,* regulation 36.
[99] *Ibid.,* regulation 37.
[100] *Ibid.,* regulation 38.
[101] *Ibid.,* regulation 40.

whether there is sufficient protection for the customer's privacy. Thus, it is time to regulate the EFT system in one body of law. This study focuses on UK Law with the objective of reflecting on the ambiguity surrounding the EFT system. One of the most significant current discussions in legal philosophy is whether the customers have sufficient protection and remedies against their banks. Existing analyses have given no comprehensive method for determining which party bears the losses in EFT risks. There are differences between one bank and another regarding the provisions made by banks for locating risks in the details of the terms and conditions of contracts. The scope of this thesis is to investigate the risk issues involved in the use of electronic payment systems. The thesis aims to explore the scope of the liability of the EFT parties for risks associated under English law. It does not aim to cover all the electronic payment methods that have been presented in the last two decades. In fact, the aim is to summarize the most significant issues which have emerged with regard to electronic payments and then to address the liability for both parties to the EFT transaction, namely, banks and customers. The thesis therefore focuses on the four points below:

First, EFT users are exposed to various types of unauthorized transaction risks, for example, fraud and, stolen or misused cards. Unauthorized EFT instruction exists when a person who does not have the right to initiate a fund transfer instruction does so. If the unauthorized instruction issued by the offender is passed, then one of the parties involved in the unauthorized transactions will bear the risk, even if there is no wrongdoing on the part of that party and all reasonable care and skill was employed. Where that risk eventually resides will depend on a sophisticated set of payment rules that rely further on: the status of

the person without the authority; the quality and type of security procedures used to process the instruction; and the instruments used to issue the EFT instructions. Section 7 of the Electronic Communications Act 2000 states:

> "(1) In any legal proceedings-
>
> (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
>
> (b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.
>
> (2) For the purposes of this section an electronic signature is so much of anything in electronic form as-
>
> (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and
>
> (b) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.
>
> (3) For the purposes of this section an electronic signature incorporated into or associated with a particular electronic communication or particular electronic data is certified by any person if that person (whether before or after the making of the communication) has made a statement confirming that-
>
> (a) the signature,
>
> (b) a means of producing, communicating or verifying the signature, or
>
> (c) a procedure applied to the signature, is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both."

This provision makes it clear that electronic signatures, supporting certificates and the processes whereby such signatures and certificates are created and used may be admitted as evidence in legal proceedings. Although the reference to "in any legal proceedings" at the start of the section might suggest that it applies only to court documents, explanatory note 44 indicates that the section allows electronic signatures to be used as evidence with regard to any

question involving the authenticity or integrity of an electronic communication or data.

Section 7 also makes it clear that it is a matter for the court to evaluate the legal effect of an e-signature in any individual case by deciding whether it has been correctly used and what evidential weight it should be given.[102] The Electronic Communications Act 2000 does not provide a statutory definition of a signature, which might assist in deciding whether or not e-signatures are to be considered as signatures in the traditional sense.[103] Instead, the 2000 Act effectively incorporates the existing common law relating to signatures. As discussed in more detail below, case law has drawn analogies between handwritten signatures and other types of authentication in terms of their functions. Applying this "function approach", English courts now recognise e-signatures as the legal equivalent of manual signatures.[104]

Although there are laws that specifically address the issues of fraud and other legal problems within internet banking and funds transfers, not much attention has been given to the area of remedies. In this era of high-end technology, it is necessary to review and re-examine unauthorized risk processes within the EFT transactions. This thesis will argue that the rules of contract law and agency law applied to EFT transactions lead to uncertainty and unpredictability regarding the EFT's parties' rights, obligations and liabilities. A further conclusion is that the bank should be liable for authenticated but unauthorized payment instructions when it is executed by a third party without the payer's

[102] *Goodman v J Eban Ltd* [1954] 1 Q.B. 550.
[103] *Ibid.; Firstpost Homes Ltd v Johnson* [1995] 1 W.L.R. 1567.
[104] Full discussion, see chapter three, section 3.3.2.3.

negligence or fault. The contention of this thesis is that it is time to propose different rules for allocating the risk of unauthorized EFT transactions.

Secondly, there is always a credit risk for both banks and customers. All customers of banks are exposed to the risk of the insolvency of their bank and the risk of the bank defaulting to execute payment transaction. The payee bears that insolvency risk if it parts with its value after EFT completion. In contrast, the payer's bank bears that risk if it guarantees the EFT payment, regardless of EFT types, even though the customer's account is inadequate. The payer, on the other hand, bears that insolvency risk before EFT completion. Finality of the EFT payment and the legal nature of payment methods are essential keys to determining which party bears the risk of insolvency. This thesis demonstrates that completion of EFT transactions has special criteria and differs from one case to another and thus the question of payment completion in the context of EFT has differing answers.

Thirdly, there are now numerous bank records full of sensitive customer information in the form of electronic data. The growth of EFT makes it possible for banks to execute increasingly sophisticated analyses of their customers' saving and spending habits, which enable banks to market their own products more effectively, but also provide a potentially very valuable source of information for third parties, such as Credit Reference Agencies. Consequently, consumer protection has become a central concern, especially with regard to privacy and the capacity of the banks to employ protection systems which are efficient in safeguarding customers' confidential data. The conclusion reached in this thesis is that there is a lack of uniform or harmonizing legislation in the procedures for data exchange and that the customer's consent is therefore the

essential key to the transmission of customer information. There is a further conclusion that consent for the passing of customer information should be subject to certain conditions. Therefore it is important to have an approved model to regulate and clarify the principles and conditions of customer data exchange.

The bank's duty of confidentiality implies a legal obligation to maintain the customer's information securely. In *Tournier v National Provincial and Union Bank of England,*[105] the Court of Appeal identified the principles of a bank's duty of confidentiality. In this case the defendant bank disclosed to its customer's employer, plaintiff's employer, the fact that one of the customer's unpaid cheques was drawn in favour of a bookmaker's account. Consequently, the customer's employer did not renew his employment contract with the customer. The plaintiff sued the bank for slander, and for breach of an implied contract that the defendants would not disclose to third persons the state of the plaintiff's account or any transactions relating thereto.[106] The outcome of case was that confidentiality was an implied term in the customer's contract and that any breach could give rise to liability in damages if loss results. Thus the decision was to the plaintiff (customer).

In *Tournier* the court held that the bank's duty of confidentiality covers all customers' information about themselves and their accounts obtained by the bank, irrespective of the information source and for as long as the banker-customer relationship exists. A bank's duty of confidentiality is not absolute, and is subject to four exceptions, identified in *Tournier*: (1) disclosure by compulsion

[105] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461 at 427.
[106] *Ibid.*

of law; (2) disclosure under duty to the public interest; (3) disclosure under the bank's own interest, and (4) disclosure under the customer's approval. The first two qualifications mean that the disclosure of a customer's private data may be required by law in cases where the public interest prevails, as the bank has no power to avoid the rules of law and will be liable if the revelation does not occur. Disclosure under the public interest has been described as 'the difficult and comprehensive meaning of the *Tournier* qualification'.[107] These difficulties could be due to a lack of clarity regarding the circumstances which would create exceptions in the public interest. Disclosure under the bank's own interest is the third exception to the bank's duty of confidentiality identified by *Tournier*. The fourth qualification in *Tournier* is the customer's consent, which may be either explicit or implicit. In *Tournier*, the court held that the best instance of a customer's implicit approval for the revelation of confidential information is where he authorizes the bank to provide a reference. This approach has been adopted by the banking sector for years.[108] However, it is sensible not to assume that a customer who provides his bank details when applying for a credit card is giving implicit approval for the disclosure of confidential information by the bank. *Tournier* has therefore been exposed to criticism in this respect.

Fourthly, the scope of the bank's liability for direct damages, consequential damages, interest losses and currency exchange losses in the context of EFT transactions is uncertain and unpredictable.

[107] Hapgood, et al., *op.cit.,* p.159.
[108] *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] A.C. 465 at pp. 503-540.

This study will demonstrate that the absence of a comprehensive statute dealing with the EFT system leads to unpredictability and uncertainty in the parties' liability for the risks associated with EFT transactions. For that reason this thesis argues that there is a need for particular rules to regulate EFT systems. Furthermore, applying the rules of contract law and agency law are insufficient to provide the final solution to the legal problems associated with EFT transactions. The essential objectives of this thesis are:

First, to address the EFT parties' liability for unauthorized EFT payment and in particular to allocate the liability for authenticated but unauthorized payment instruction. Identity authentication in the context of EFT is a problem, because it is difficult to determine whether the payment instruction is authorized or not. Such difficulty is related to the absence of a physical meeting between the bank and customer. This thesis will show that applying the existing law, namely contract law and agency law, leads to the problem of customer identity. The banks are obliged to install effective encryption methods available for the prevention of unauthorized access to accounts and for the safeguarding of their own and the customers' interests. Any avoidable shortcomings in these security measures will result in the bank's liability. That is because the bank is in control of the security procedures which are used by the customers. Thus, the bank cannot obtain benefit of the flaw in the machinery that customers are required to use. Therefore, it is reasonable to consider a bank liable for an authenticated but unauthorized transaction when the payer acted without fraud or gross negligence and he denies issuing such a transaction.

Secondly, to address the exact time of the completion of EFT payments and to identify the party who bears the risk of insolvency. In EFT transactions there are

a number of parties and functions presumed by every party that could be affected by the time of the payment. This thesis will show that, regarding the question of 'finality of EFT payment,' different answers should be adopted. The PSR 2009 present new rules for irrevocability of payment instruction and execution time of payment instructions. Nevertheless, they do not resolve the question of when the EFT should be considered final.

Thirdly, to address the banks' liability for safeguarding its customer's confidential information. Security means the protection of the integrity of EFT systems and their information from illegal or unauthorized access and use. It is important to address whether banks employ encryption systems which sufficient to keep customers' information confidential and to protect electronic transactions data. This thesis will demonstrate the need for a new legal approach and the need for this approach to be comprehensive in the context of a bank's duty of confidentiality in EFT transactions. Further, due to the EFT system's development, the banks have to take all reasonable care to provide very high security procedures to prevent any attack or unauthorized access to the banks' accounts and transactions and the customer's electronic data.

Fourthly, to address the bank's liability to the customer for direct damages and consequential damages. The most common disputes arising from EFTs involve unauthorized payment and failures or delays in transfers. Damages attributable to these breaches or delays may include losses to the principal amount of the transaction when the payer's bank debits his account due to unauthorized instruction. Furthermore, the payer will not be able to use that amount of money for his own business purpose because it is no longer in his account. Accordingly, the payer may lose favourable contracts or sustain financial loss as

a penalty for later payment. Further, the payer will lose the interest he would have been paid for that amount of money if it had still been in his account. The payer may also lose the fees he paid to the payer's bank to make the fund transfer to a specific payee and the money instead may be transferred to a fraudster. Finally, there are losses resulting from foreign exchange rate fluctuations between the expected and actual time of receipt funds transferred. Resolution of these disputes requires the determination of party liability for the losses. The remedy of consequential damages, interest and currency exchange losses in the context of EFT is uncertain and unpredictable.

The conclusion is that the PSR 2009 are a positive but insufficient step towards addressing all the uncertain issues surrounding EFT transactions. This thesis concludes that customer protection is the essential factor in the regulation of EFT. There is a lack of uniform or harmonized legislation applicable to existing EFT. Also, the thesis concludes that there is a deficiency in the existing law to determine which party bears the risk of unauthorized transaction, insolvency and disclosure of confidential information. Thus, it is time to conceive a different method to approach risk-allocation rules in the EFT system. There are new proposals for legal provisions to regulate EFT completion, authenticated but unauthorized instructions, privacy and recoverability of damages in cases of EFT losses. Although with the continuing evolution of electronic banking the suggested, regulations may not provide a comprehensive answer, they will address most of the salient issues and could play a major part in providing remedial solutions.

1.4 Questions raised by the research

Traditionally, the monitoring measures, laws and regulatory norms associated with banking procedures were designed primarily to address safety and transparency issues within the functioning of financial institutions. To create a process that is safe for the customers and well protected from losses arising from a lack of adequate legal remedial processes is of the utmost importance for a successful banking operation, which by its very nature handles large amounts of money, and thus is classed as 'high-risk' business practice. The high risks associated with banks comprise mainly credit-interest risks, law related issues, and insolvency risks. Internet banking and the EFT system has further increased these risks while creating some new ones, which may arise from the banks' attempts to circumvent regulatory and supervisory norms in order to expand their customer reach.[109] Other risks of a legal nature stem from the ambiguities of various legal processes and the fact that regulations vary from one country to another.[110] The main question that the thesis aims to answer is: which party bears risk of losses in cases of unauthorized transactions, authenticated but unauthorized transactions, insolvency and disclosure of customers' private information. The thesis also argues the need to regulate the EFT system in a more consistent manner.

In order to address this question, the research also answers secondary and associated questions, such as: What is the legal nature of an EFT instruction?

[109] Bollen, European regulation of payment services – the story so far, *op.cit*., pp. 454-455.
[110] Mthembu, M. A., 'Electronic Funds Transfer: exploring the difficulties of security', (2010) 5 (4) *Journal of International Commercial Law and Technology* 201 at p.201.

What is the legal validity and recognition of electronic signatures as a signature? What is the liability of certification authorities and electronic signatures? When is an EFT payment considered final? What is the legal nature of a plastic card payment? Is the bank's duty of confidentiality absolute? Does the bank's duty of confidentiality fall under the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950? Does the bank have the right to disclose its customer data to the Credit Reference Agencies? Finally, in the case of EFT losses, does the bank bear both direct damages, and consequential damages or one of these, or neither?

1.5 Methodology and structure of the thesis

EFT has changed the nature of the risks associated with funds transfers. EFTs create new risks which by virtue of their novelty have not yet been well understood, and even when understood have not yet been well regulated. The aim of this thesis is to examine the scope of the liability of the banks and customers for insolvency, unauthorized payment and disclosure of customers' private information in the context of EFT under English law. The thesis's main academic reference point is the intersection between law and practice. This study methodology is to analyse, investigate and evaluate existing English law in order to assess whether it is sufficient and appropriate in regard to the legal risks currently associated with EFT transactions. It provides a clear and authoritative explanation of the law governing EFT in the UK. It helps identify the practical legal questions likely to arise and explains how to deal with them effectively. Analysis of the latest case law is a particular feature of this study, as

the courts address the uncertainties created by the new technology. Recent judgments from the UK are explained throughout the text. The thesis addresses key areas of contention, such as the legal nature of funds transfer, completion of EFT payment, EFT parties' liabilities, liability for authenticated but unauthorized transactions, the problem of customers' identity, data protection in an electronic context and damages for recoverable EFT losses. It deals with newly emerging areas of importance, such as encryption, data protection and disclosure of customers' private information to the Credit References Agencies. It also includes coverage of the UK implementations of the PSD 2007 and the E-Signatures Directive. This will be done by examining and assessing the PSR 2009 compared with the general principles of agency law, contract law and the rules which apply to forged cheques in English law. Finally, it deals with bank practice, as evidenced by examination of the general contracts terms and conditions published by Barclays, Lloyd's TSB and HSBC. Important judgments are examined. [111] The study puts forward recommendations for future approaches to determining parties' liabilities in EFT transactions and proposes model rules for the protection of customers' rights in EFTs.

The thesis is divided into seven chapters. The first chapter is devoted to the background of the EFT clearing system, the legal EFT framework and serves as a general introduction. Chapter two is devoted to identifying the basic legal concepts and important definitions involved in the EFT system and clears the way for a fuller analysis in subsequent chapters. The chapter starts by defining

[111] For example, *Libyan Arab Foreign Bank v Bankers Trust Co* [1989] Q.B. 728; *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194; *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461; *Derry v Peek* (1889) 14 App. Cas. 337; *Hadley v Baxendale* [1854] 9 Ex. 341.

the EFT system in relation to the aims of the present study. It describes different forms of payment instruction and different categories of EFT. The essential legal implications of EFT instructions, such as sources of law, the legal status of an EFT instruction, and the contractual relationship created by such an instruction are clarified. It is emphasized that an understanding of the legal nature of EFT instructions helps to build a proper regulatory regime for what are often conceptually difficult products.

Chapter three deals with a long standing issue in banking transactions: unauthorized EFT instruction. The basic motivation behind such transactions is fraud. This chapter finds out how the application of the common law rules of agency to EFT creates the issue of identity authentication due to the idiosyncratic nature of authentication in the EFT instruction. Chapter three analyses the existing laws that cover unauthorized EFT transactions, namely the common law rules and the PSR 2009. The authorization and carrying out of EFT instructions are governed by the PSR 2009 Part 6, consisting of Regulations 51-79. These regulations also establish rules governing the parties' duties and obligations in the transactions. This chapter will argue that the laws are insufficient or inefficient in addressing the problems associated with unauthorized EFT. This chapter will also examine whether banks are obliged to have a high security system in EFT to protect customer's accounts and funds. The legal position of the security procedures and the security methods used to authenticate EFT are investigated in this chapter. Finally, chapter Three will determine which party bears the risk in an unauthorized transaction and which party will bear the losses in the case of authentication of unauthorized EFT instructions.

A tracking of the process of an EFT transaction is described in chapter four. Among the bank's duties to its customers is executing the payment instruction and making the payment to the payee. Chapter four attempts to find out the exact time of an EFT transaction by carrying out an analysis of current EFT principles. An analysis of EFT completion time is also carried out, via an investigation of the PSR 2009 and the common law rules. The different rules and principles used to point out the exact time of payment completion will be assessed, the comparative and conflicting points will be analysed and comprehensive ways of resolving the deficiencies in the current regulations will be suggested.

An EFT is completed at the destination bank in the system chain in a credit transfer and the payment operation is completed at the payee's bank. Conversely, in a debit transfer the payment operation is completed at the payer's bank. To achieve the purpose of this chapter it is important to examine the legal nature of electronic payment methods. The legal nature of a payment can be conditional, as in payment by debit card, or it can be an absolute payment, such as in credit card payments. Finally, by identifying the time of payment completion this chapter will examine the liability of the risk of insolvency in EFT transactions and will address the question of which party will bear the losses.

Chapter five attempts to investigate the bank's duty of confidentiality, as it is one of the main obligations of a bank to its customer. Some problems that are related to legal validity, liability and customer protection, particularly where a hacker gains entry to accounts, are discussed in this chapter. Furthermore, there are some circumstances when the bank has the right to disclose a

customer's confidential information or data. The purpose of this chapter is to examine these problems, along with the present laws and regulations relevant to the EFT system, and to discover how they can be used to regulate the EFT's main legal issues. The investigation will also show that the banks face an increasingly complicated task in reconciling and balancing their different obligations with regard to information and details pertaining to their customers, given that, customers may have significant expectations about banking confidentiality. Therefore, it is argued, in future both the jurisdiction and the government should not further extend the rules or qualifications regarding the duty of confidentiality without taking into account all the consequences of the general laws of confidentiality and the sophistication of the electronic banking sector. Also, they will have to evaluate statements regarding misuse of confidential information and their obligations in this area, in order to make sure that the bank uses very high security systems to maintain the confidentiality of customer information.

In the EFT transaction, where a bank is held responsible for a breach of one or more of its contractual obligations, a customer may request compensation. Accordingly, chapter six attempts to show what measure of losses are applicable in the different circumstances of a bank's breach of their obligations within EFT. This principally involves the execution of an EFT instruction according to unauthorized instructions, the banks' insolvency and defaults in making EFT payments or disclosure customer's private data without legal authority. Where there is no regime to measure losses or damages, common law rules will be invoked to express an estimate of losses in particular circumstances where banks breach their obligations.

Chapter seven is a summary and a conclusion drawn from the chapters cited above. It includes most but not all of the present author's views and also, model proposals and recommendations, although views and recommendations can also be found in the other chapters. This chapter's main aims are to recall and highlight the significant issues and to suggest means of resolving such issues. The significant issue which this concluding chapter attempts to address is the deficiency of the existing law; therefore the necessity for a particular regime dealing with the EFT system will be discussed therein.

Chapter Two

Legal Aspects of EFT System

2.1 Introduction

The definition of EFT is the starting point for any work on the subject, since the parameters of the discussion in this thesis will depend greatly on such a definition. EFT means the movement of an amount of money from a customer's bank account to another's bank account by electronic means.[1] Such a transfer is classified as either a non-consumer activated EFT or a consumer activated EFT.[2] Also, EFT is classified as either a credit transfer or a debit transfer. A non-consumer activated EFT means the bank activates the payment, through CHAPS Clearing Company, for example, which is either a credit transfer or a direct debit, while a consumer activated EFT means the customer activates the payment, for example in a payment by card. Consumer activated EFT is always described as a debit transfer order.[3]

This thesis is devoted to the study of the rights, obligations and liabilities for losses and the risks of customers and banks in the context of EFT transactions. The function of this chapter is to present an overview of the legal aspects of EFT transactions. To achieve this aim the chapter will be divided into five sections. Section 2.2 will spell out the essential legal definition of an EFT

[1] Arora, A., *Electronic Banking and the Law* (1988), p. 7.
[2] Saxby, S., *Encyclopaedia of Information Technology Law* (1990), Ch. 5.
[3] Further details, see Hapgood, M., et al., *Paget's Law of Banking* (2007), p. 354.

instruction. EFT terminology will be discussed in section 2.3. This section will analyse the terminology of the United States Uniform Commercial Code (UCC) and UNCITRAL and compare it with the terminology used within the PSR 2009. Section 2.4 explores the significance of the different categories of EFT. Finally, section 2.5 is devoted to examining the legal implications of EFT. Section 2.5.1 examines the law as it applies to an EFT transaction. Section 2.5.2 explains and clarifies plastic card contractual schemas. Section 2.5.3 will examine the legal nature of EFT under common law to determine how the law applies to EFT transactions. This section will conclude that the legal nature of funds transfer is neither an assignment, nor a negotiable instrument, and does not create trust funds. Instead, an EFT is merely a mandate from the customer to the bank. In this regard, comprehension of the legal nature of an EFT helps to build a proper regulatory regime for what are often conceptually difficult products.[4] Section 2.6 will summarize the main findings of this chapter, which notes that EFT transactions are subject to different legal rules, for example, the rules of contract law, agency law and the PSR 2009. The existing law, however, does not provide final answers to all the legal uncertainties arising in the EFT context.

2.2 Definition of EFT

English law does not give a specific definition of the concept of payment in a general sense. Goode suggests a commonly accepted definition of payment as: "a gift or loan of money or any act offered and accepted in performance of a

[4] Bollen, R., 'A discussion of best practice in the regulation of payment services: part 2', (2010) 25 *International Banking Law and Regulation* 429 at p. 439.

money obligation".[5] According to this definition, a payment is not always money but can also be some other form or action of exchange between the two parties involved in a transaction. Thus, any action accepted by the payee in enactment of a money duty can be considered payment. With regard to EFT there is no particular definition, EFT means replacing paper-based payment orders with electronic methods to authorize a building society, bank or other financial institution to credit or debit a customer's account.[6] Geva[7] has defined the payment mechanism in the following words: 'any machinery facilitating an electronic payment in monetary value; while authorizing or granting the payee the right to request the fund transfer from the third party, it permits the payer (1) to escape the transfer of funds in the physical delivery; (2) where applicable, to obtain a settlement between the payer to the payee'. The Jack Committee has defined EFT as follows:[8]

> "a funds transfer effected through the banking system by electronic techniques, with input and output methods being largely or completely in electronic form"

By this definition the significant difference between paper-based fund transfer and EFT is the way the payment instruction is created. EFT transactions are

[5] Goode, R., *Payment Obligations in Commercial and Financial Transactions* (1995), p. 501.
[6] Arora, *op. cit.,* p. 7.
[7] Geva, B., 'Payment finality and discharge in funds transfers', (2008) 83 *Chicago-Kent Law Review* 633 at p. 635; Geva, B., *The Law of Electronic Funds Transfers* (2003), s. 1.03[1]; Geva, B., *Legal Aspects Relating to Payment by E-Money: Review of Retail Payment System Fundamentals* (2001), p. 11; Geva, B., 'The concept of payment mechanism', (1986) 24 *Osgood Hall Law Journal* 1 at p. 4.
[8] *Report by the Review Committee on Banking Services: Law and Practice*, ("The Jack Report") (1989, London, HMSO, Cm 622), p. 75.

initiated by a payment instruction from the customer to his bank to transfer, or collect, money from one bank account to another by electronic devices.[9]

EFT orders, whether debit transfer orders or credit transfer orders, are initiated by using off-line or on-line electronic devices.[10] The Jack Committee considered an Electronic Funds Transfer at Point of Sale (EFTPOS hereafter) to be a means of transferring money from the payer's account to the payee's account by use of the payer's payment via his card at the payee's cash point to obtain goods, services or cash as an on-line EFT.[11] Recently it has become possible to transact EFTPOS via a mobile phone.[12]

Both non-consumer activated EFT and consumer activated EFT fall within the ambit of this thesis. Any EFT transaction is initiated by a payment instruction which could be transmitted, directly or indirectly, from the customer to a bank by giving an order either to transfer or collect a fixed amount of funds to a payee's bank which does not state a condition of payment to the payee other than time of payment. By this definition, a payment instruction has several features: first, the purpose of the payment instruction is the payment, which is either collected directly or is awaiting collection, and in which the sum of money must be fixed. Secondly, the payment instruction must be unconditional, although the customer is free to determine the time of payment.[13] Thirdly, the payment

[9] Ellinger, E., et al., *Modern Banking Law* (2011), p. 562; Sappideen, R., 'Cross-border Electronic Funds Transfers through large value transfer system, and the persistence of risk', (2003) 13 *Journal of Business Law* 584 at p. 585.
[10] Geva, B., 'International Funds Transfers: Mechanisms and Laws', in Chris, R., et al., *Cross-Border Electronic Banking, Challenges and Opportunities* (2000), p. 6.
[11] *Review Committee on Banking Services: Law and Practice*, *op.cit.,* p. 77.
[12] UKPA, *Payment Council* http://www.paymentscouncil.org.uk/media_centre/press_releases/-/page/2041/ 20 April 2013.
[13] Part 2 (3)(1) of Bill of Exchange Act 1882 states "A bill of exchange is an unconditional order".

instruction has to be addressed to a bank or financial institution.[14] Therefore, a funds transfer addressed to an individual does not constitute an EFT instruction. A final element of the EFT instruction is that an electronic payment always depends on the transfer of money from a debtor's bank account to the creditor's bank account, irrespective of whether by a debit transfer system or by a credit transfer system. Recently, with the implementation of the PSR 2009 a payment order is defined under regulation 2(1) as "any instruction by (a) a payer; or (b) a payee, to their respective payment service provider requesting the execution of a payment transaction". This definition governs both funds transfer types, credit transfers and debit transfers, and it is the definition adopted in this thesis.

Electronic transfer of funds from one bank account to another, whether intra-branch (accounts held at the same branch of the same bank), inter-branch (accounts held at different branches of the same bank), or inter-bank (accounts held at different banks). If the EFT transaction is passed it will result in the debiting of the payer's account by the payer's bank; the transfer of funds by the payer's bank to the payee's bank; the acceptance by the payee's bank of the transfer whereby the payee's bank is indebted to the payee; and the crediting of the payee's account by the payee's bank'. In brief, EFT replaces the payer's debt by making the payee's bank indebted to the payee instead of the payer. Any shortcoming in these procedures will give rise to the liability of one of the transaction's parties. Therefore, it is important to address each point of proceedings to determine the liability, for example, the point at which EFT payment to be considered final to allocate the liability of the bank's insolvency.

[14] Hapgood, et al., *op.cit.,* p. 354.

2.3 EFT terminology

Before 2009 some attempts were made in the UK to standardize the terminology of the EFT. They were largely influenced by article 4A of the UCC. The UNCITRAL Model Law on Credit Transfer 1992 has adopted the same terminology as the UCC. However, article 4A of the UCC, which was adopted in 1989, describes credit transfer instructions only. [15] Further, the same terminology in article 4A and The UNCITRAL Model Law on Credit Transfer was adopted in the Credit Transfer Directive on Cross-Border Credit Transfers,[16] and within UK law, in 1999, with the implementation of the Directive 1997 through the Cross-Border Credit Transfer Regulations 1999; [17] the same terminology has been adopted. The Cross-Border Credit Transfer Regulations 1999 are limited in scope, covering only cross-border credit transfers[18] of not more than 50,000 euros or the equivalent in another European Economic Area

[15] The Prefatory Note to article 4A is explained the terminology of the EFT as follows: "X, a debtor, wants to pay an obligation owed to Y. Instead of delivering to Y a negotiable instrument such as a check or some other writing such as a credit card slip that enables Y to obtain payment from a bank, X transmits an instruction to X's bank to credit a sum of money to the bank account of Y. In most cases X's bank and Y's bank are different banks. X's bank may carry out X's instruction by instruction Y's bank to credit Y's account in the amount that X requested. The instruction that X issues to its bank is a 'payment order'. X is the 'sender' of the payment order and X's bank is the 'receiving bank' with respect to X's order. Y is the 'beneficiary' of X's order. When X's bank issues an instruction to Y's bank to carry out X's payment order, X's bank 'executes' X's order. The instruction of X's bank to Y's bank is also a payment order. With respect to that order, X's bank is the sender, Y's bank is the receiving bank, and Y is the beneficiary. The entire series of transactions by which X pays Y is known as the 'funds transfer'. With respect to the funds transfer, X is the 'originator', X's bank is the 'originator's bank', Y is the 'beneficiary' and Y's bank is the 'beneficiary's bank'. In more complex transactions there are one or more additional banks known as 'intermediary bank's between X's bank and Y's bank. In the funds transfer the instruction contained in the payment order of X to its bank is carried out by a series of payment orders by each bank in the transmission chain to the next bank in the chain until Y's bank receives a payment order to make the credit to Y's account".

[16] The Cross-Border Credit Transfer Directive (1997 OJ L43/25).

[17] The Cross-Border Credit Transfer Regulations 1999 (SI 1999/1876).

[18] *Ibid.*, regulation 2(1).

currency. In 2007 the Credit Transfer Directive was replaced by the PSD,[19] which was adopted into English law through the PSR 2009. Part 5 and 6 deal with information required from the banks or any other financial institution to their customers involved in EFT transactions falling within their ambit, and the regulations explain clearly the rights and duties of the parties.[20] PSR 2009 presents a novel terminology which differs from that of the Cross-Border Credit Transfer Regulations 1999 (Figure 1, page 48), and the same terminology applies to both credit and debit transfer instructions.[21] Accordingly, the terminology used in the PSR 2009 is as follows: the term payer is used to refer to the customer who initiates, or consents to, the initiation of the payment instruction; while the term payee refers to the person who is the intended recipient of funds which have been the subject of a payment instruction[22] (Figure 2, page 48).

Given the above descriptions, it seems that the points of comparison between the terminology used in the UCC and UNCITRAL with the terminology used in the PSR 2009 could be as follows:

(A) The UCC and the Cross-Border Credit Transfer Regulations 1999 used the term originator to refer to the customer who initiates, or consents to the initiation of the payment order, while the term beneficiary referred to the person who is the intended recipient of funds which have been the subject of a payment order. In the PSR 2009 the term payer is used to refer to the customer who initiates, or consents to the initiation of the

[19] PSD (2007/64/EC).
[20] PSR 2009, regulation 2(1).
[21] *Ibid.*
[22] *Ibid.*

payment instruction and the term payee refers to the person who is the intended recipient of funds which have been the subject of a payment instruction.

(B) The terminology employed in the Cross-Border Credit Transfer Regulations 1999 provides a more useful and comprehensive terminology insofar as it not only covers international instruments and domestic legislation in other jurisdictions but is also specific to the context of EFT, whereas the terminology of the PSR 2009 is general and is applicable to both electronic and cash payments.

(C) Nonetheless, the terminology presented in the PSR 2009 is much more comprehensive in scope than its predecessor. The Cross-Border Credit Transfer Regulations and UUC terminology restrict the term “fund transfer” to credit transfers and it does not apply to debit transfers, although the Cross-Border Credit Transfer Regulations use the same terminology for both credit and debit transfers. By contrast, the PSR 2009 terminology applies to both credit and debit transfers.

Accordingly, to achieve the aims of this thesis the terminology used in the PSR 2009 has been adopted. The term “payer” will be used to refer to the customer who initiates, or consents to the initiation of the payment order. The term “payee” will refer to the person who is the intended recipient of funds which have been the subject of a payment order. Furthermore, the term “payer’s bank” will refer to the bank which moves the funds and the term “payee’s bank” will refer to the bank which requests the funds. Also this thesis will use the terms “correspondent” or “intermediary” bank to refer to any intermediary institutions.

Figure 1: The Cross-Border Credit Transfer Regulations and UCC terminology.

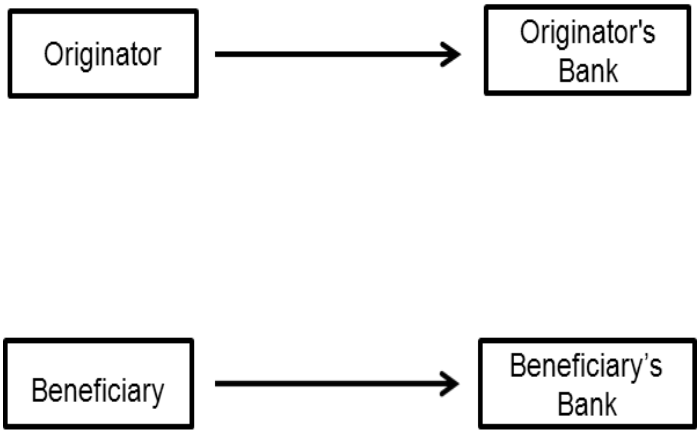
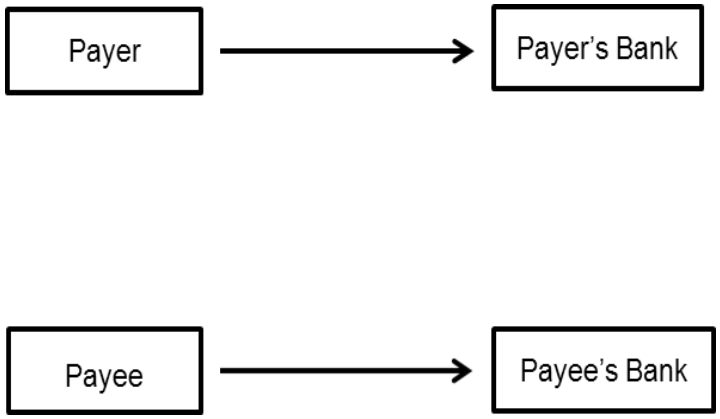


Figure 2: The PSR 2009 terminology.



2.4 EFT systems categories

An EFT is classified as a credit transfer or a debit transfer,[23] and secondly, as either a non-consumer-activated EFT or a consumer-activated EFT.[24] A non-consumer-activated EFT or wholesale EFT transaction means the bank activates the payment through a large value transfer system such as BACS,

[23] Further, see Goode, R., *Commercial Law (*2009), pp. 504-505.
[24] Saxby, *op.cit.,* Ch. 5.

CHAPS and Faster Payment. A consumer-activated EFT or retail transaction means it is the customer who activates the payment, which in most cases is a debit transfer order, effected by using a card, for example, or some form of internet payment, or via a mobile phone.[25] A retail EFT transaction or consumer-activated EFT, such as one involving payment by cards, is used to make a transaction by which the customer obtains goods or/and services and at the same time makes a payment by card, the funds being transferred electronically from the cardholder's account to the merchant's account.[26] Therefore, a consumer-activated EFT contains a different contractual agreement and each agreement is governed by a separate contract.[27]

2.4.1 Credit and debit transfers

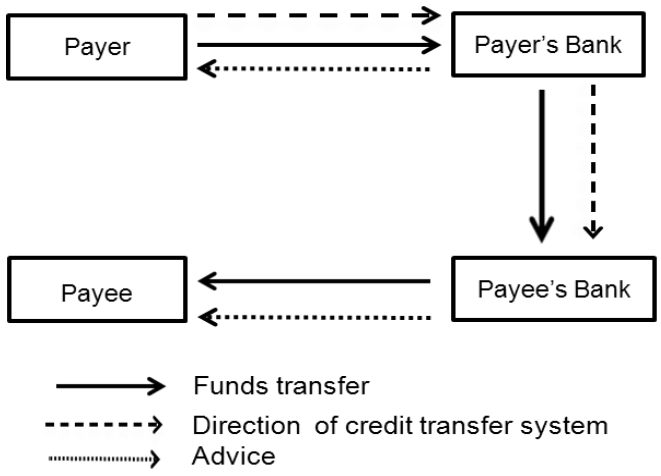
A funds transfer by any electronic device involves the payee's acceptance of the transaction settlement by means of such a device. Therefore, the payee's bank must be clearly identified and there must be no ambiguity about the address at which the transaction's funds are credited to the payee's account.[28] The payee's bank replaces the payer's obligation: this replacement is due to the payer creating a payment instruction and such an instruction being accepted by the payee's bank.[29] Consequently, payment is made despite the payee's bank not actually crediting the payee's account: accepting the payment instruction is

[25] Hapgood, et al., *op.cit.,* p. 354.
[26] Robinson, D., 'The structure and Characteristics of the Principal Electronic Banking system', in Goode, R., *Electronic Banking: The Legal Implications* (1985), p. 1.
[27] See section 2.5.2 of this chapter.
[28] Geva, *International Funds Transfers: Mechanisms and Laws*, *op.cit.,* p. 8.
[29] *Ibid.*

sufficient for the payment to be considered final.[30] EFT systems can be categorized either as credit transfers or as debit transfers, depending on the way in which the payment instruction is transferred to the payer's bank.

A credit transfer instruction is initiated by the payer who orders his bank to move funds from his account to the payee's bank account.[31] Thus, the payer's bank moves the amount of the transaction to the payee's bank by some form of credit transfer, such as a standing order or payment instruction initiated through the internet banking system. On receipt of the payer's payment instruction, the payer's bank account is debited and the payee's bank account is credited when the payee's and payer's accounts are held at same bank or a payment instruction is forwarded to the payee's bank, which will then credit the payee's account (Figure 3 below).

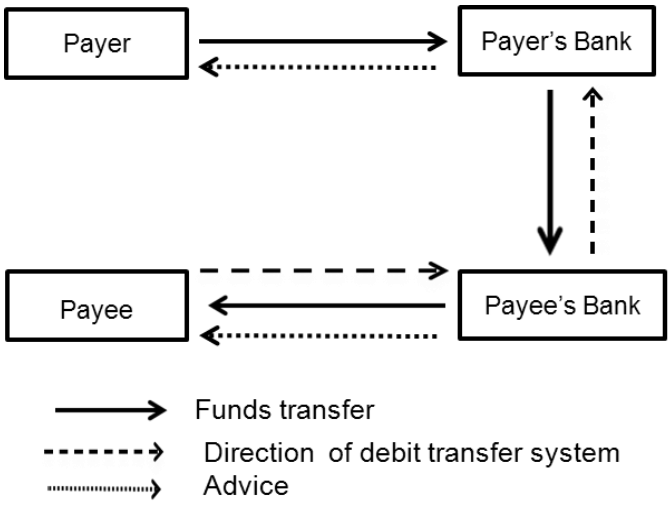
Figure 3: Credit transfer system.



[30] See chapter four.
[31] Ellinger, et al., *op.cit.,* p. 562; Cox, R. and Taylor, J., 'Funds Transfers', in Brindle, M. and Cox, R., *Law of Bank Payments* (2010), p. 57; Hapgood, et al., *op.cit.,* p. 361.

Conversely, a debit transfer instruction is initiated by the payee, who asks his bank to request the funds from the payer's bank account, for example as a direct debit. A debit transfer instruction can be initiated by the payer and passed on to the payee, as for instance in a payment by cheque.[32] On receipt of the payee's order, the payee's bank usually credits the payee's account provisionally with the funds to be withdrawn and then forwards orders to the payer's bank. Subsequently the payer's account will be debited. The transfer of funds to the payee's account is actually considered final when the debit to the payer's account becomes irrevocable (Figure 4 below).

Figure 4: Debit transfer system.



[32] Goode, Commercial Law, *op.cit.,* p. 504; Ellinger, et al., *op.cit.,* p. 562.

2.4.2 Non-customer-activated EFT systems

The four basic clearance methods operating in the UK are: the C&CCC; BACS; CHAPS;[33] and the 'Faster Payments Services'. Together these systems, for all of which liability is currently divided between four independent companies operating under the auspices of the UKPA.[34] C&CCC is paper-based, involving the manual transmission of giro forms and is similar to the clearing of cheques. The other three methods: BACS, CHAPS, and 'Faster Payment Schemes Limited' involve electronic clearing. Nevertheless, the clearing techniques are basically a matter of practice rather than of law, although certain aspects of the procedure involved are relevant for defining the legal roles assumed by the practice.

2.4.2.1 Clearance via BACS

BACS are clearances of small and medium-value funds transfers, either by debit transfers, such as standing orders, which are used largely by individuals for the payment of regular fixed sums, or credit transfers, such credit being used mainly for the disbursement of regular bulk payments such as salaries and wages.[35] Furthermore, BACS is used for other transactions, such as one-off payments to business suppliers and to pass customer payments initiated via

[33] Ellinger, et al., *op.cit.*, at p.577; Kolodziej, A., 'Customer-banker liability in electronic banking', (1986) 7 *Journal of Company Lawyer* 191 at p. 191.
[34] These companies are Cheque and Credit Clearing Company (C&CCC); Bankers' Automated Clearing Services Limited (BACS); Clearing House Automated Payment System (CHAPS); and Faster Payments Scheme Limited.
[35] Bank for International Settlements, 'Payment systems in the United Kingdom', in *The Red Book* (2003), p. 4.4 http://www.bis.org/publ/cpss53p14uk.pdf 17 July 2013.

internet or telephone. Finally, interbank transfers, originating from direct debits, allow recipients of large numbers of payments. Processes are cleared via BACS, for example, allowing insurance companies and service utilities to collect these payments automatically from bank or building society accounts. The great advantage of using the BACS system is that it enables fund transfers without the need for paper work or for actual transmission of documents. The BACS clearing procedures normally used to take three days and this was the main criticism of such a method.[36] However, the PSR 2009 stipulated that from 1st January 2012 the BACS clearing procedures time must change from three days to one day.[37] BACS thereafter employed the sophisticated CHAPS 'Faster Payments Services', which presents a near-real time or same day service. Presently there are 16 BACS members.[38] Each member has immediate access to the BACS system and offers BACS with credit and debit payment orders as electronic messages for processing.[39] However, users have the right to sponsor their customers, for example, non-member banks, building societies and corporate customers, who are not members of BACS, permitting them to transfer their own electronic messages to BACS. Liability, however, remains with the member and not with the sponsored customer.

[36] Cox and Taylor, *Funds Transfers*, *op.cit.,* p. 83.
[37] The PSR 2009, regulation 70(1) and (2).
[38] For a list of present members, see http://www.bacs.co.uk/bacs/corporate/corporateoverview/pages/ourmembers.aspx 15 February 2012.
[39] Ellinger, et al., *op.cit.,* p. 579; Hapgood, et al., *op.cit.,* p. 377.

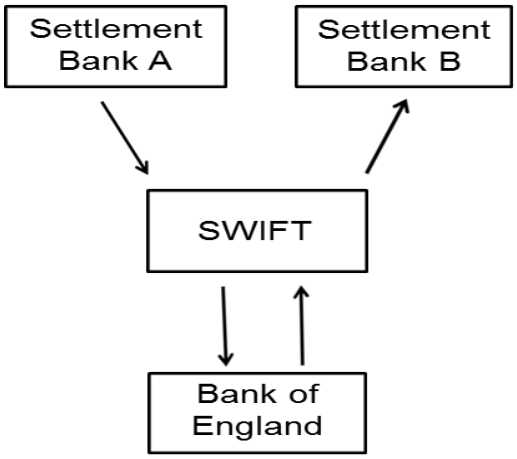
2.4.2.2 Clearance via CHAPS

CHAPS payment is an electronic bank-to-bank; same-day funds transfer made within the UK in sterling, and is generally used for high-value interbank transactions.[40] CHAPS Euro went live on 4 January 1999 and provided a high-value clearing for euro-denominated payments running over SWIFT. On 28 August 2001, CHAPS Sterling and CHAPS Euro were consolidated into a 'New CHAPS' system. But, CHAPS Euro closed on 16 May 2008 just prior to TARGET2 going live. One quadrillion pounds processed through CHAPS following a payment of £500 million made on 25 July 2011.[41] Statistics show that the total value of EFT cleared via CHAPS for 2012 was £7.7 trillion.[42] The main advantage of CHAPS is that it is fast, since the money is transferred on the same day. CHAPS funds transfer orders are irrevocable. CHAPS Sterling is one of the largest real-time gross settlement (RTGS) systems in the world. Banks themselves use CHAPS to move money around the financial system, but it is normally used for other types of funds transfer, such as business-to-business funds transfers, and also by people buying or selling a high-value item. CHAPS allows its member banks access to TARGET2, which are the payment operations for cross-border and inter-bank data using the sophisticated uniform system of the International Organization for Standardization run by the Society for Worldwide Interbank Financial

[40] UKPA, http://www.ukpayments.org.uk/payment_options/chaps/-/page/203/ 5 February 2013.
[41] UKPA, *CHAPS Clearing Company*, 2010 http://www.chapsco.co.uk/chaps_company/about_chapsco/-/page/1971/ 15 February 2013.
[42] UKPA, *CHAPS Statistic* http://www.chapsco.co.uk/about_chaps/chaps_statistics/ 13 September 2013.

Telecommunication, 'SWIFT'.[43] According to the CHAPS Scheme Rules, payments made through CHAPS must be unconditional,[44] and furthermore a payment message cannot be revoked from the point at which the members' settlement account is debited[45] (Figure 5 below).

Figure 5: Funds movement through CHAPS Sterling system.



2.4.2.3 The Faster Payments Service

The Faster Payments Service was the first new payment service to be presented in the UK for more than 20 years.[46] By the end of May 2008 most banks had started offering the new Faster Payments Service for online banking and phone payments. Accordingly, standing orders began to be processed using the new service. PSR 2009 stipulates that from the beginning of 2012 all fund transfers must reach the payee's account by the next working day after the

[43] Universal Financial Industry Message Scheme www.iso20022.org 13 September 2013.
[44] CHAPS Clearing Company, *CHAPS Scheme Rules* (Version 10, July 2013), rule 3.1.2 http://www.chapsco.co.uk/files/chaps/governance_documents/chaps_co_rules.pdf 18 July 2013.
[45] *Ibid.,* rule 3.2.1.
[46] UKPA, http://www.fasterpayments.org.uk/faster_payments/about_faster_payments/-/page/1941/ 15 February 2013.

customer has initiated the EFT order.[47] To ensure that this service is available to all customers, all members that currently accept BACS funds transfers give an assurance that they are able to accept standing orders, phone and online banking payments through Faster Payments.[48] The new maximum time schedule for EFT, technically known as Day+1, requires payments to reach the payee's account by the end of the next working day. Nevertheless, all standing orders, cards payment and phone banking payments in the UK will exceed this requirement, being processed end-to-end within two hours through the Faster Payments service.[49]

The liability of the Faster Payments scheme is limited to the day-to-day procedures and management of the service.[50] Also, it is limited to covering four methods of payment orders: first, 'instant payments' for when the payer wants to make a single credit funds transfer immediately; secondly, 'forward-dated payment' for when the payer wants to make single credit funds transfer but not at the present time; thirdly, 'standing orders'[51] whereby the payer gives his bank a mandate to pay the same recipient the same amount at regular intervals;[52] and finally, 'Corporate Bulk' payments, which are files of BACS funds transfer data that can be submitted to the Faster Payments Service for funds transfer on the same day. It seems that there are several dissimilarities between the 'Faster Payments Service' and the other clearances system types. The most significant

[47] PSR 2009, regulation 70(1)(2); Also, see UKPA, Payments Council http://www.paymentscouncil.org.uk/media_centre/press_releases/-/page/1995/ 15 February 2013.
[48] PSR 2009, regulation 70(1)(2.).
[49] UKPA, Payments Council, *op.cit.*
[50] *Ibid.*
[51] Before the 'Faster Payments Service' standing order is carried out via PACS.
[52] UKPA, Faster Payments 2011. http://www.fasterpayments.org.uk/faster_payments/how_to_use_the_faster_payments_service_new/-/page/1947/ 15 February 2013.

dissimilarity between the 'Faster Payments Service' and the BACS payment is the speed of the funds transfer operations. BACS has a three day payment cycle, while the 'Faster Payments Service' gives same day clearance based on the methods of payment order involved. Furthermore, 'Faster Payments Service' is used for instant and forward-dated payments, 24 hours a day, seven days a week, although standing orders are only processed between midnight and 6.00 a.m. on business days.[53]

2.4.3 Consumer-activated EFT systems

When the customer selects a particular method to use in the EFT systems it is often referred to as a consumer-activated EFT or retail EFT.[54] In this thesis, consumer-activated EFT systems refer to payment by cards, internet payments and payment by mobile phone. Credit cards, charge cards, debit cards, which are known as EFTPOS, ATM cards, and prepaid cards, will also be within the ambit of this thesis. [55] Cheque cards out of scope of this thesis because in 2011 it stopped for using. According to the UKPA, Payment Council, the UK Domestic Cheque Guarantee Card Scheme closed on 30 June 2011 cheque cards means:

> "A cheque guarantee card was a plastic card that was used with a cheque as a guarantee to the recipient that the payer's bank would pay them the value of the cheque, provided that the cheque was legitimately presented by the account holder and accepted by the payee in accordance with the conditions of use of the Scheme. The card confirmed the payer's identity

[53] UKPA, *op.cit.*
[54] Heller, S., 'A proposal for consideration of a unified payments law', (2009) 83 *Chicago-Kent Law Review* 485 at p. 488; Hapgood, et al., *op.cit.,* p. 354.
[55]http://www.paymentscouncil.org.uk/current_projects/cheque_guarantee_card_scheme/what_is_a_cheque_guarantee_card/-/page/1526/ 16 February 2012.

> and guaranteed a sum up to the limit marked on the cheque card. The limit was normally £50 or £100, but 12% of cards carried a £250 guarantee limit. It was not possible to place a stop on a guaranteed cheque and once the bank received the cheque they would have had to pay it".

Debit and credit cards are the most frequently used payment methods because of the lack of commercial obstacles to their use.[56] These methods of payment are used comprehensively for retail payments. Statistics on the use of plastic card payments shows that in 2010 total spending by this method was £353 billion; by 2011 the figure had grown to £379 billion,[57] and in 2012 it had increased to £478.6 billion.[58]

2.4.3.1 Credit cards

The first credit card issuer in the United Kingdom was Barclaycard in 1966.[59] Credit cards supply their customers with multifarious benefits. They authorize the holder to obtain goods and/or services as well as cash.[60] Credit cards classify as credit-tokens and so are regulated by section 14(1) of the Consumer Credit Act (CCA) 1974 which defines a credit token as:

> "a card, check, voucher, coupon, stamp, form, booklet or other document or thing given to an individual by a person carrying on a consumer credit business, who undertakes—(a) That on the production of it (whether or not some other action is also required) he will supply cash, goods and services(or any of them) on credit, or (b) That where, on the production of

[56] Hornle, J., 'The European Union takes initiative in the field of e-commerce', (2000) 3 *Journal of Information Law & Technology* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/hornle 31 May 2012.
[57] UKPA, *The UK Card Association Annual Report 2012*, Card Expenditure Statics at p. 1 http://www.theukcardsassociation.org.uk/files/ukca/ces_montly_updates/2011/dec_11_commentary_full.pdf 06 February 2013.
[58] *Ibid.*
[59] UK Cards Association http://www.theukcardsassociation.org.uk/Advice_and_links/index.asp 25 May 2013.
[60] Ellinger, et al*., op.cit.,* p. 649.

> it to a third party (whether or not any other action is also required), the third party supply cash, goods and services (or any of them), he will pay the third party for them (whether or not deduction any discount or commission), in return for payment to him by the individual".

The overall common aim for a credit-token is to enable the card holder to obtain goods, services and /or cash by using a card or often a token.[61] A consumer credit transaction refers to any purchase and sale and therefore the provision of credit within a regulated consumer credit agreement is necessary. A credit card is also issued under a credit-token agreement, [62] which is a transaction between the debtor and the supplier [63] under a debtor-creditor-supplier agreement regulated by the CCA, section 12(b).[64]

Under section 14(b) of the CCA 1974, usage of a credit card creates a tripartite relationship between the card issuer, the card holder and the trader. [65] Occasionally the card holder is given a cheque book, thus the card holder's account can be used in a classical bank transaction as well.[66] When the card holder wants to obtain cash through the use of an ATM there are two parties involved, rather than the three normally present in other kinds of credit token transactions.[67] Thus, the card holder's account is debited electronically while the card holder is receiving his cash from the ATM. Finally, the PSR 2009 is not applicable to the credit cards issued within CCA, because PSR 2009 is merely a reiteration of the CCA 1974 provisions.

[61] Hapgood, et al., *op.cit.,* p. 83.
[62] CCA 1974 Section 11(4).
[63] *Ibid.*, section 189(1).
[64] *Bank of Scotland v Alfred Truman* [2005] EWHC 583 (QB) at pp. 586-587.
[65] Lambert, J., *Banking the Legal Environment* (1993), p. 140.
[66] Macleod, J., *Consumer Sales Law* (2002), p. 60.
[67] CCA section 14(a)(1).

2.4.3.2 Charge cards

The use of charge cards is limited mainly to transactions involving entertainment, thus they are often called ‘‘Travel and Entertainment (T&E) Cards.’’ [68] The procedures for charge cards use are the similar to credit card, except that the holder is not entitled to cash withdrawal facility and must liquidate the balance in one payment.[69] As a result of the adoption of the Consumer Credit Directive,[70] currently charge cards fall under section 14 of the CCA 1974. They are predominantly governed by the Act and are otherwise governed by the PSR 2009. Before the implementation of the Consumer Credit Directive, there was no doubt that charge cards generally gave rise to ‘exempt agreements’[71] and hence the cards fall outside the ambit of CCA1974 and did not give rise to credit-tokens and credit-token agreements.[72] Nevertheless, the Consumer Credit (Exempt Agreements) Order 1998 was incompatible with the Consumer Credit Directive 2008. It is no longer available and therefore charge cards now fall within the ambit of section 14 of the CCA 1974 and give rise to credit-token agreements.[73] Thus the same rules described in relation to credit cards apply here.

Charge card payment takes place when the order to the card issuer is given by filling in the relevant payment boxes on the provider’s website checkout and the suppler will gain authorization of the order, that is, the card issuer’s confirmation

[68] Sayer, P., *Credit Cards and the Law: An Introduction* (1988), p. 5.
[69] Hapgood, et al., *op.cit.,* p. 84; Sayer, *op.cit*., p. 5.
[70] Consumer Credit Directive 2008 (2008/84/EC), which implemented in the UK by adopting the Consumer Credit (EU Directive) Regulation 2010 (SI 2010/1010).
[71] Article 3(1)(a)(ii) of the Consumer Credit (Exempt Agreements) Order 1998 (SI 1989/869)
[72] Ellinger, et al., *op. cit*., at p. 655 and 665; Cox and Taylor, Funds Transfers, *op.cit.,* p 250 and 284.
[73] Ellinger, et al., *op.cit.,* at pp. 665-666.

that it will honour the order (which will generally be given if the transaction is within the cardholder's charge card and the card is not suspected to be stolen), while the cardholder is still online to the checkout page.[74]

2.4.3.3 Debit cards

The use of debit cards or EFTPOS[75] has grown rapidly in the last twenty years. This form of electronic service offers the rightful holders access to their bank account at any time and from any geographic location in the world. [76] Such access is possible via the use of plastic cards issued by the bank in the holder's name and can be used at the point of purchase, at a cash point machine, at the bank or via telephone transaction.[77] Debit card payment works by authorizing the holder either to make retail payment at the point of obtaining goods and services or to obtain cash via ATM.[78] The security of the transaction is assured by issuing customers with personal identification numbers (PINs). [79] This ensures that the card and the PIN belong to the rightful holder through a comparison of the card's details and the bank's customer account, and used in this way the PIN acts as a mandate to the bank for payment.[80] When the rightful holder uses a PIN to make a purchase the debit will be on his or her current

[74] Smith, J. H. G., et al., *Internet Law and Regulation* (2007), p. 879.
[75] Geva, B., 'The E.F.T. debit card', (1989) 15 *Canadian Business Law Journal* 406 at p. 406; Kolodziej, *op.cit.,* p. 192; further, see Review Committee on Banking Services: Law and Practice, *op.cit.,* p. 77.
[76] Smith, M., and Robertson, P., 'Plastic Money' in Brindle, M. and Cox, R., *Law of Bank Payments* (2010), p. 214.
[77] Akindemowo, E., 'Contract, deposit or e-value? reconsidering stored value products for a modernized payments framework', (2009) 7 *Business & Commercial Law Journal* 275 at p. 302.
[78] Smith and Robertson, *op.cit.,* p.226; Caskey, J. P., et al., 'Is the debit card revolution finally here?', (1994) 4 *Economic Review* 79 at p.80; Kolodziej, *op.cit.,* p.192.
[79] Since 14 February 2006 rightful holders demand to recognise their PINs.
[80] Hapgood, et al., *op.cit.,* p. 393.

account, so the card holder's account must always be kept in credit.[81] When a debit card is used, the payer's account and the payee's account are settled by debit and credit messages sent electronically over the network.[82] Debit cards are also used to obtain goods and/or services through mail order or telephone transactions. In these types of transactions the card holder gives the payee some security information, and the payee must save this information for his records.[83] There are two basic debit cards schemes in operation in the UK, Visa Debit (owned by Visa), and Switch/Maestro, run by Maestro Card Services Ltd.[84]

Most commercial law commentators[85]argue that debit cards are credit token agreements regulated by the Consumer Credit Act (CCA) 1974 when there is an overdraft facility, but not when there is no overdraft agreement. Overdraft is a contract to provide a customer with an overdraft facility which is called a running-account credit.[86] An overdraft facility on a card holder's bank account will often be an unrestricted-use credit contract which means it is not made within a pre-existing agreement with any sellers. Therefore it is a debtor-creditor agreement.[87] So with an overdraft facility a debit card agreement falls under the definition of a credit-token agreement.[88] Debit cards do not fall under sections 56 and 75 of the CCA 1974 because they are not considered to involve a

[81] *Ibid*., at p. 83; Rosenthal, D., *Guide to Consumer Credit Law and Practice* (1994), p. 97.
[82] Hapgood, et al., *op.cit.,* p. 393.
[83] Geva, *The Law of Electronic Funds Transfers, op.cit.,* p. 198.
[84] The Office of Fair Trading, *First annual progress report of the Payment Systems Task Force,* (2005), p. 26 http://www.oft.gov.uk/shared_oft/reports/financial_products/oft789a.pdf 06 February 2012.
[85] Goode, R., *Consumer Credit Law and Practice* (loose-leaf), paras [25.83]-[25.84]; Guest, A., and Lloyd, M., *Encyclopaedia of Consumer Credit Law* (1975), para 2-015; Hapgood, et al., *op.cit.,* pp. 83-84; Caux, T., et al., *Electronic Banking and Treasury Security* (2000), pp.8-9; Smith and Robertson, *op.cit.,* p. 286.
[86] CCA 1974, section 10(1) (a).
[87] *Ibid.*, section 13(c).
[88] *Ibid.*, section 187(3)(a).

"debtor-creditor-supplier" agreement in accordance with which the debit card issuer will not be responsible for any misuse by the seller. Hapgood, et al,[89] however, state that debit cards are not credit-token agreements, but should be regulated under the debtor-creditor-supplier agreement[90] because the holder obtains goods or services from the seller and pays from his bank account. He suggested that credit token agreements are to be defined as "regulated agreements" so that debit cards are just a method of payment and outside the ambit of the CCA 1974. Since credit is drawn by the debit card user from the card issuer at the point of purchase the relationship between the card holder and the card issuer falls under section 14(3) CCA, so it is difficult to argue that debit cards do not fall under the CCA 1974.[91] Section 14(3) of the CCA 1974 specifies that the issuer of cards is obliged to guarantee the payment to the suppliers (third party) every time the cardholder receives goods, services or cash. Under Section 14(2) of CCA 1974, the above relationship falls under credit-token agreements. Not all agreements where a credit token is issued fall within the definition of credit token agreements; not all debit card issues, for example, are accompanied by an overdraft account. Whether debit cards are to be considered as credit tokens or as credit token agreements is a matter which remains open to debate. The author's view is that debit cards fall outside the ambit of the CCA 1974. Thus, the issuer of the card is under no obligation to guarantee the payment and make the transaction when there are insufficient funds in the cardholder's account and there is no overdraft facility. Secondly,

[89] Hapgood, et al., *op.cit.,* pp. 83-84.
[90] CCA 1974, section 12.
[91] Hapgood, et al., *op.cit.,* at p. 84.

debit card holders are not protected by the CCA 1974 rules, which would, for example, enabe the card issuer to obtain chargeback.

Within the PSR 2009 the situation is different. It seems that the PSR 2009 covers payment by debit cards as well as payment by all other types of cards, since debit cards are held to fall within the definition of a 'payment instrument' created under a payment services contract. [92] Therefore, the debit card holder is subject to protection under the PSR 2009.[93] Also it covers the parties' rights, liabilities and duties.[94] It is important to note a possible conflict between the CCA 1974 regulations and those of PSR 2009 with regard to payments by card, such as in case of misuse of the card.[95] Solving that conflict simply by applying the CCA 1974 to the obligations and liabilities of cards issues in relation to 'regulated agreements' and the PSR 2009 will not be applicable, because PSR 2009 are merely a reiteration of the CCA 1974 provisions.[96]

2.4.3.4 ATM cards

In 1967 the first cash machine in the UK was introduced by Barclays Bank.[97] An ATM card enables the holder to obtain cash only, so it is not a credit device. The cardholder uses the card by inserting it into the machine and typing his Personal Identification Number (PIN). Holders of ATM cards can use the card only in the ATM of the cards issuing bank or the ATMs of other banks with

[92] PSR 2009, regulation 2(1).
[93] *Ibid.*, Part 5.
[94] *Ibid.*, Part 6.
[95] See chapter three, section 3.4.1.
[96] PSR 2009 regulations 34 and 52.
[97] UK Cards Association http://www.theukcardsassociation.org.uk/Advice_and_links/index.asp 25 July 2012.

whom the issuing bank has reached an agreement.[98] However, most banks and building societies issuing ATM cards are members of networks using shared ATMs, such as LINK in the UK.[99] The PSR 2009 regulations apply to ATM cards and cover the agreement between the cardholder and the issuing bank.[100] However, the PSR 2009 do not cover the relationship between the cardholder and another bank or building society which owns the ATM used by the cardholder.[101] ATM cards do not fall under the CCA 1974, and there is disagreement over the classification of ATM cards as credit tokens.[102]

2.4.3.5 Prepaid cards

Prepaid cards, or stored value cards, involve the storing of monetary value as electronic data outside of a bank account. Thus, the prepaid card holder may obtain an account for only a relatively small proportion of payments of lower value such as bus and tube fares. Prepaid cards can be equivalent to credit or debit cards and many of these cards are created under the aegis of Maestro, MasterCard, or Visa. Further, a number of prepaid cards can be purchased, loaded with a low value and used until the money on the card is spent. Others are re-loadable and can be 'topped-up'.[103] The closest equivalent to a prepaid

[98] Smith and Robertson, *op.cit.,* pp. 262-263; Sealy, L.S., and Hooley, R.J.A., *Commercial Law* (2009), p. 810.
[99] UKPA, Payments Council http://www.paymentscouncil.org.uk/who_do_we_work_with/payments_schemes/link/-/page/1151/ 25 July 2012.
[100] PSR 2009, Schedule 1 Part 1 Para 1(b).
[101] *Ibid.,* Schedule 1 Part 1 Para 2.
[102] See section 2.4.3.1.
[103] UK Cards Association, *op.cit*.

card is cash rather some other type of card.[104] The prepaid card is an electronic value which the holder uses with his money for goods and/or services purchased from a seller involved in the scheme. In contrast, with a credit card it is the card's issuer who pays for goods and/or services each time it is used by the holder, and at that same time the holder will be indebted to the issuer. Finally, prepaid cards do not fall under the CCA 1974, but under the PSR 2009.

[104] E-Money Directive 2009 (2009/110/EC) particularly text in article 13 that e-money in view of its character as an electronic surrogate for coins and banknotes.

Table 1: Attributes and examples of cards payment.

Attributes	**Credit Cards**	**Charge Cards**	**Debit Cards**	**ATM Cards**	**Prepaid Cards**
Account	Bank account	Bank account	Customer current account	Customer current account	No bank and customer account
Value	Limited value	Limited value	Unlimited value	Limited value	Limited value
CCA 1974 Applicable	Yes	Yes	No	No	No
PSR 2009 Applicable	Yes	Yes	Yes	Yes	Yes
Functions	1- Withdraw money 2- Pay for goods and services 3- Cash back	Pay for particular services	1- Withdraw money 2- Pay for goods and services 3- Cash back	Withdraw money only	Pay for particular services
Acceptance	Yes	Payee must agree to use	Yes	Issuing bank or any ATM of LINK network	Payee must agree to use
Examples	Visa Credit, MasterCard, and American Express	American Express cards	Visa Debit, MasterCard, and Visa Electron	ATM cards	Visa and MasterCard

2.5 The essential legal implications of EFT instructions

2.5.1 Sources of law

In the context of a modern banking system using the internet, “electronic banking” or “e-banking” is defined as a banking operation conducted by authorized banks from a remote location through tools that function under the bank's direct management or through outsourced agents. Thus, e-banking encompasses an entire set of processes through which a customer can transfer funds electronically without having to visit a bank physically. These processes also include services where customers can access their accounts, conduct personal or business transactions and receive on the internet necessary information on different financial services and products.

In the UK, the lack of comprehensive regulation governing EFT means that EFT transactions come under the jurisdiction of the law of contract and the law of agency. Although the PSR 2009 is considered to be the most significant legislation dealing with EFT when the EFT falls within the 2009 Regulations,[105] the Financial Markets and Insolvency (Settlement Finality) Regulations 1999 also apply.[106] The Regulations 2009 present new rights for customers regarding such matters as, for example, charges, execution time and the revocability of payment instructions, while the Financial Markets and Insolvency (Settlement

[105] See chapter one, section 1.2.4.

[106] The Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (SI 1999/2979), (as amended), which replaced the Settlement Finality Directive (98/26/EC) of the European Parliament and of the Council on settlement finality in payment and securities settlement systems.

Finality) Regulations 1999 address issues related to safety of the payment procedures and securities payments in the event of the insolvency of a payment party.

2.5.1.1 Law of agency

The established legal view of the banker-customer relationship in relation to EFT is that it is an agent- principal relationship.[107] There is consensus[108] in the literature that the bank acts as an agent to its customers in carrying out transactions. The importance of the law of agency in EFT is demonstrated through the decision of Webster J. in *Royal Products v Midland Bank*.[109] The litigants were Royal Products, which had a current account with the defendants, Midland Bank and also with the Bank of Industry, Commerce and Agriculture Ltd, (BICAL) in Malta. Royal Products gave an order to the Midland Bank in UK to transfer £13,000 from their current account there to their current account with BICAL in Malta. However, BICAL was facing insolvency problems at that time. The Midland Bank therefore wanted to avoid involvement in the legal issue and used the Bank of Valletta (National) in Malta as its intermediary to transfer £13,000 to BICAL. National subsequently transferred the funds to BICAL, informing them that the funds were to be credited to Royal Products' account. The next day BICAL became insolvent and failed to credit the £13,000 to Royal Products' account. Consequently, Royal Products sued Midland on the grounds

[107] Chorley, L., *Law of Banking* (1974), Ch. 3; Cox and Taylor, Funds Transfers, *op.cit.,* p. 124.
[108] Hapgood, et al., *op.cit.,* p. 406; Ellinger, et al., *op.cit.,* p. 126 and 601; Arora, A., 'Contractual and tortious liability in EFT transactions in the United Kingdom', *op.cit.,* p. 291, Cox and Taylor, *Funds Transfers*, *op.cit.,* p. 124.
[109] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 at p. 198.

that, if National was not the agent of Midland then their order was never executed, which meant that Midland was liable; but if National was acting as an agent of Midland, then National broke essential obligations and duties of a fiduciary nature, for breach of which Midland was liable. In this case, the decision of Webster, J. was for Midland.[110] With regard to the relationship between the payer and the payer's bank, Webster, J. held that the legal implication of the payment instruction given by the customer to the bank was only a mandate and the relationship between the payer's bank and its customer is that of agent-principal and governed by agency law. Accordingly, one of the bank's duties as its customer's agent was strict adherence to the customer's mandate. Therefore, as the funds transfer was addressed to Midland Bank as part of the banker-customer relationship, Webster, J. held that Midland was under a duty to exercise all reasonable skill and care in executing the customer's instruction, and that National acted as Midland's agent. The court held that an agency relationship existed between the payer, Royal Products, and the payer's bank, Midland. Additionally, an agency relationship existed between Midland and National, the intermediary. Webster, J. held:

> "in carrying out its part of the transaction Midland owed Royal Products a duty to use reasonable care and skill…. and that they would be vicariously liable for the breach of that duty by any servant or agent to whom they delegated the carrying out of the instructions. Midland, therefore, would be liable to Royal Products for National's negligence, if any, in that respect. But in my judgment National owed no duty of any kind direct to Royal Products….. In my judgment, therefore, National are not to be regarded as having been agents of Royal Products and did not, therefore, owe them any of the duties, including a fiduciary duty, owed by an agent to his principal."[111]

[110] *Ibid.*, at p. 201.
[111] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 at p. 198.

Nevertheless, there was an absence of agency relationship between the payer, Royal Products, and the intermediary bank, National. The court held that in spite of the fact that Midland acted as an agent to Royal Products and that Midland was entitled to employ National to effect the fund transfer, Midland was not capable of creating any relationship between Royal Products and National. Accordingly, National was under no duty at all to Royal Products, not even fiduciary duties.[112]

2.5.1.2 Law of contract

The second legal view of the banker-customer relationship in relation to EFT is the debtor-creditor relationship.[113] This relationship is founded on the fact that the customer's funds deposited in the bank's account are owned by the bank, which the customer has to claim from the bank as a creditor. When the customer's account is in credit the customer will act as creditor to the bank, and conversely the bank acts as creditor when the customer's account is debited or overdrawn**.**[114] Although, in *Royal Products v Midland Bank* the court held that the Midland's contract with Royal Products was not specifically a contract to supply a fund transfer only, the two parties were, nevertheless, held to be in a contractual agreement because of their underlying relationship as a bank and customer, the payer bank normally charging the payer a fee to issue a fund

[112] *Ibid.*
[113] *Foley v Hill* (1848) 9 E.R. 1002, this case has been approved later in *Joachimson v Swiss Bank Corporation* [1921] 3 K.B. 110; Further, see Bollen, R., 'A review of the development and legal nature of payment facilities' (2005) 16 *Journal of Business and Law* 93 at p.105.
[114] *Foley v Hill* (1848) 9 E.R. 1002.

transfer on the payer's behalf.[115] In each case, the terms and conditions of the contract between the parties will be significant in determining the duties and the obligations for both parties. In this regard, the payer's bank normally excludes liability for the negligence or default of its correspondent in its contract with the customer.[116]

2.5.2 Plastic cards contractual schemes

As explained previously, there are different types of plastic card payments and every type will involve a network of agreements, some involving a tripartite agreement,[117] (figure 6, page 75), recently, with the development of card payment networks, the contractual schemes have come to involve four parties: the card holder, the issuer, the merchant and the merchant acquirer.[118] Indisputably, these agreements will depend on the issuer's terms and conditions, and these will differ from one issuer to another.[119] They include the agreement between the card holder and the card issuer, the agreement between the merchant and the card issuer and the agreement between the merchant and the card holder. In a tripartite agreement each party has two agreements in the transaction.[120]

[115] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 at p. 209.
[116] Cox and Taylor, Funds Transfers, *op.cit.,* p. 126.
[117] Sealy, *op.cit.,* p. 833.
[118] *Office of Fair Trading v Lloyds TSB Bank Plc* [2008] 1 A.C. 316; Further, see Shy, O., and Tarkka, J., 'The Market for Electronic Cash Cards', (2002) 34 *Journal of Money, Credit & Banking* 299 at p. 302; Lowe, R., *Commercial Law* (1983), p. 472.
[119] Akindemowo, *op.cit.,* pp. 311-312.
[120] *Re Charge Card Services Ltd* [1987] Ch. 150 at p. 158 C-D.

2.5.2.1 Agreement between the card holder and the card issuer

Normally this contract entitles the issuer to pay for the holder's transactions.[121] This contract requires information from the card holder, such as: the holder's name and address, the sum of money involved and other details.[122] With the debit card scheme the position is different the terms and conditions for use of debit cards are included within the general terms and conditions for the bank account.[123]

2.5.2.2 Agreement between the merchant and the card issuer

There is a contractual agreement between the merchant and the card issuer, based on the relationship between them.[124] Generally, this contract will contain a form giving details of which cards the seller is entitled to accept for the settlement.[125] On the one hand, the card issuer accepts liability for paying the card holder's transactions[126] while on the other hand the merchant burdens the card issuer to pay the merchant on the basis of the contract between them.[127] Under the contract between merchant and issuer the merchant cannot refuse to sell goods and/or services to the holders who pay using any legally valid card.

---

[121] Smith and Robertson, *op.cit.,* p. 263.
[122] Sayer, *op.cit.,* pp. 44-45.
[123] Lloyds TSB, *Your banking relationship with us,* October 2012 http://www.lloydstsb.com/assets/media/pdfs/banking_with_us/personal_banking_terms_and_conditions.pdf; Barclays, *Customer Agreement,* March 2012, http://www.barclays.co.uk/ImportantInformation/TermsandConditions/P1242575350746; HSBC, *General Terms and Conditions,* April 2012 http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf 9 January 2013.
[124] Sayer, *op.cit.,* p. 68.
[125] Ellinger, et al., *op.cit.,* p. 653; Smith and Robertson, *op.cit.,* p. 260.
[126] Sayer, *op.cit.,* p. 68.
[127] Lord Diplock in *Commissioner of Police of the Metropolis v Charles (Derek Michael*) [1977] A.C. 177 at p. 182.

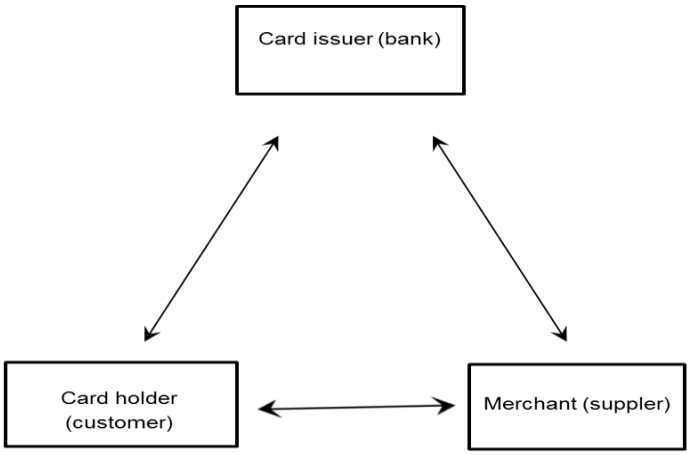
Furthermore, there is a contractual agreement between the merchant and the merchant's bank, which called the 'Merchant Agreement' and contains standard terms. According to this contract, the seller is authorized and obliged to accept the card in payment in making transactions, and the bank agrees to pay to the merchant the value of the transactions.[128]

2.5.2.3 Agreement between the merchant and the card holder

The third contract existing between the merchant and the card holder is usually oral. However, the implied conditions and terms imposed remain under the regulation of the "Sale of Goods Act 1979" or the "Supply of Goods and Services Act 1982". The rights of the payer and the payee are based on that agreement. Such a contract could be subject to the rules of either CCA 1974 or PSR 2009. Therefore, if the issuer provides a settlement to the payee, it means the card holder authorizes the issuer to pay and allows the issuer to exercise his right to draw from the card holder's account. Figure 6 overleaf describes the three party card schemes.

[128] *Re Charge Card Services Ltd* [1987] Ch. 150, at p.158.

Figure 6: The three party card schemes



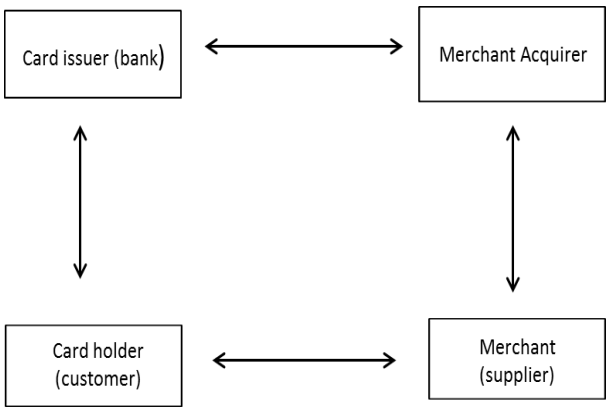
2.5.2.4 Agreement between the merchant and the merchant acquirer

The fourth type of contract (addition to the three contractual agreements explained above), under a card scheme may involve four parties. This point is illustrated by the decision in *Office of Fair Trading v Lloyds TSB Bank Plc.*[129] The House of Lords held that, in general, the contract in a credit card transaction had a tripartite structure, involving contracts between the card issuer, the cardholder and the merchant. However, with the introduction of modern electronic banking credit card schemes, this subsequently developed into a four-party structure involving a "merchant acquirer". This contract is not regulated by the CCA 1974 or PSR 2009, as the bank is free to opt out of the protection presented by Part 5 and 6 of the PSR 2009. Thus, this contract will be regulated according to the master agreements scheme by VISA and MasterCard. The purpose of a "merchant acquirer" is to recruit new sellers to

[129] *Office of Fair Trading v Lloyds TSB Bank Plc* [2008] 1 A.C. 316.

accept payment by cards (debit cards and credit cards). Modern electronic banking has driven the card issuers to become members of one or other of the two basic international cards networks, Visa and MasterCard. Within the principles of Visa and MasterCard networks (merchant acquirer), the banks (card issuers) are authorized to issue cards and normally undertake to honour the cards and payments[130] (Figure 7 below).

Figure 7: The four party card schemes.



2.5.3 The legal nature of an EFT instruction

In defining the legal nature of the payment instruction, it is of primary importance to clarify the law governing EFT contractual relationships. In addition, the law serves to address the principles and rules which can be applied to the parties' rights, obligations and liabilities. The next four sections will demonstrate that under English law the funds transfer is only a mandate

[130] *Ibid.,* at p. 325 A per Lord Mance.

initiated by the payer to his bank.[131] There will also be arguments against the suggestion that an EFT works as an assignment and also against the view that the funds transfer may be a negotiable instrument. There will also be a discussion and refutation of the view that an EFT instruction may be a device which creates a trust of funds.

2.5.3.1 An EFT instruction is not an assignment

A reading of the available literature leaves no doubt that funds transfers either by debit or credit, are involved in the settlement of the balances of the payer and the payee accounts, regardless of whether the funds transfer is within a single bank or between different banks.[132] EFT is only a transfer of value and not a transfer of money, so there is no physical transfer.[133] Respectively the payer's bank account is debited and the payee's bank account is credited.[134] Cox and Taylor have clarified that in practice, if there is no term in the contract to the contrary, the payer does not assign his rights towards the payer's bank to the payee or the payee's bank.[135] Accordingly the payment order could be revoked until the time the payment orders become irrevocable, for example, before it reaches the payee's bank, while the assignment order would be irrevocable once it is complete.[136] In *Libyan Arab Foreign Bank v Bankers Trust*

[131] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194.
[132] Hapgood, et al., *op.cit.,* p. 358; Ellinger, et al., *op.cit.,* p. 559; Cox and Taylor, *Funds Transfers*, *op.cit.,* p. 56.
[133] Ellinger, et al., *op.cit.,* p. 559; Cox and Taylor, *Funds Transfers*, *op.cit.,* p. 56.
[134] Hapgood, et al., *op.cit.,* p. 358; Ellinger, et al., *op.cit.,* p. 559; Cox and Taylor, *Funds Transfers*, *op.cit.,* p. 56.
[135] Cox and Taylor, Funds Transfers, *op. cit.,* p. 128.
[136] Arora, *Electronic banking and the law, op.cit.,* p. 51

Co[137] Staughton J. has asserted that a funds transfer is not an assignment. Staughton J.'s view has been reinforced by the House of Lords in *R. v Preddy*.[138] Staughton J. held:

> ""Transfer" may be a somewhat misleading word, since the original obligation is not assigned (notwithstanding dicta in one American case which speak of assignment); a new obligation by a new debtor is created."[139]

A funds transfer system is not a statutory assignment. Ellinger, et al.[140] have confirmed that a funds transfer system is not a statutory assignment under section 136 of the Law of Property Act 1925 for the following reasons: first, in the fund transfer the customer usually orders the bank to transfer part of the debit owed by the bank to its customer. Thus, the assignment of part of a debt is not approved by section136 of the Law of Property Act 1925.[141] Secondly, the customer may not have any outstanding credit at the time of issuing the funds transfer, as the customer believes that the amount required to complete the transaction will be available at the time the transfer is to be affected. Thus, the assignment of future funds is not recognised by section 136 of the Law of Property Act 1925.[142]

Moreover, none of the funds transfer types, for example, bank giro credit, CHAPS and EFTPOS discloses an intention to confer on the payee the right to claim payment of the amount involved from the payer's bank, as would result in the case of an assignment.[143] With regard to EFT, parties there is no intention that

[137] *Libyan Arab Foreign Bank v Bankers Trust Co* [1989] Q.B. 728 at p. 750.
[138] *R. v Preddy* [1996] A.C. 815.
[139] *Libyan Arab Foreign Bank v Bankers Trust Co* [1989] Q.B. 728 at p. 750.
[140] Ellinger, et al., *op .cit.,* p. 597.
[141] *Ibid.*, at p. 598.
[142] *Ibid.*
[143] *Ibid.*, at p. 599.

part of the debt payable by the payer's bank to the payer be made over to the payee as a chose in action claimable by him. Therefore, EFT operations work in different way, with the machinery and with the objectives pertaining to the assignment of debts.[144] Accordingly, an EFT is not an assignment and the Law of Property Act 1925, does not apply to such transactions.

2.5.3.2 An EFT instruction is not an negotiable instrument

Section 3 of the Bill of Exchange Act 1882, enshrines the requirements for a funds transfer instrument to be a negotiable instrument: first, it must be an "unconditional order" in writing; second, it must be addressed by one person to another, and thirdly, ordering the addressee to pay on demand or at a fixed or determinable future time a specific amount of money to the payee. Regarding the former requirements, negotiable instruments are considered to consist of a paper which passes from one party to another, either by delivery or by indorsement, as a result of which that negotiable instrument itself becomes the subject of payments transfer or negotiation. Thus, the funds transfer such as cash and EFT is not negotiable instrument.[145] EFT falls outside the ambit of definition of a negotiable instrument, as it is not a written order by the customer to his bank to transfer or collect funds from one account to another by electronic means. This is well illustrated by the decision in *The Brimnes*[146] in which the Court of Appeal held that the legal nature of a funds transfer order conferred by

[144] This view has been supported by Ellinger, et al., *op cit.,* p. 599; Cox and Taylor, Funds Transfers, *op.cit.,* p. 128
[145] Ellinger, et al., op. cit., at pp. 595-596; Cox and Taylor, Funds Transfers, *op.cit.,* at p. 132.
[146] *Tenax Steamship Co Ltd v Brimnes (Owners of), The Brimnes* [1975] 1 Q.B. 929.

a telex message could not be a negotiable instrument, so that a telex could not be equivalent to a cheque, Cairns L.J. held:

> "The property in money passes on delivery; so does the property in a cheque. Partly by operation of the law merchant and the Bills of Exchange Act 1882, partly by the customs of business, cheques have come to be regarded as the equivalent of money (subject always to being afterwards defeated by dishonour). I do not think that the telex message in this case can be regarded in the same way. It was not a negotiable instrument. It could have been revoked by Hambros [the payer's bank] at any time before being acted on by M.G.T. [payee's bank], and, if it had been so revoked, no action could have been brought on it as it could on a stopped cheque."[147]

Furthermore, a negotiable instrument's contract creates explicit rights which are separate from the underlying agreement which has been made and an EFT does not do this. Regarding to EFT, the payer instructs his bank to pass funds from his account to the payee's account pursuant to the underlying agreement between them, and yet the payee cannot hold that the instruction gave him rights and that the payment is considered made.[148] Thus, as an EFT is not a real transfer on demand or within a determinable time, it becomes a transfer once the payer has created the payment instruction.[149]

Although, an EFT is not considered to be a negotiable instrument, in *Esso Petroleum Co Ltd v Milton*,[150] the claimant, the occupier of a petrol service station, was required to pay for his petrol deliveries by direct debit arrangements with his bank. The claimant cancelled his direct debit mandate when £170,000 was still outstanding for petrol previously delivered by the defendants. The Court of Appeal held that the payment arrangements of the

[147] *Ibid.,* at p. 969.
[148] Sealy, *op.cit.,* p.526.
[149] Ellinger, et al., *op.cit.,* p.596.
[150] *Esso Petroleum Co Ltd v Milton* [1997] 1 W.L.R. 938.

parties by direct debit were to be treated as same as payment by cheque, and the claim was the same as that of a payee who had no guarantee of a cheque's payment. It was submitted that an EFT instruction (direct debit) was equivalent to payment by cheque and, a fortiori, equivalent to payment by cash. The Court of Appeal held:

> "modern commercial practice was to treat payments by direct debit in the same way as payments by cheque and the equivalent of cash."[151]

However, Cox and Taylor[152] disagreed with this view and they confirm that if the Court of Appeal is right, this point 'could be applied to payment made, or agreed to be made, by other forms of credit and debit transfer between bank accounts. Furthermore, a funds transfer instruction does not embody any contractual rights arising from the underlying transaction, and the payee in an EFT transaction is not possessed of a right to payment. Hence, EFT instructions fall outside the definition of a negotiable instrument, since EFT instructions are not payments at a particular date or on demand. Further, EFT instructions are not payments on the instructions of a particular individual or to the bearer. Finally, EFT instructions do not often include words which can be construed as a formal instruction passed from the payer to his bank.

[151] *Ibid.,* at p. 939.
[152] Cox and Taylor, Funds Transfers, *op.cit.,* p.133.

2.5.3.3 An EFT instruction does not create trust funds

There is no doubt that an amount in a bank account can from the matter of law a trust fund. An EFT instruction does not give explicit trust of the funds which are intended for transfer because the use of the word trust is not sufficient in itself for a trust to issue, there must also be the intention to create a trust.[153] So in a case where a payer becomes insolvent before the payment order is effected, the payee will be on the side of ordinary unsecured creditors, since there is no intention to create trust funds when the bank is ordered to transfer the amount to the payee. In *Re Kayford Ltd (In Liquidation)*[154] the court held that a trust of the funds in a bank account has been found are far removed from cases involving a funds transfer order. Therefore, in *Re Kayford Ltd* the order by the account holder to the bank was to create a "Customer's Trust Deposit Account". Moreover, the clear intention was to safeguard the customers, whose fund was paid into the account, in the event of the insolvency of the account holder. In an ordinary EFT instruction, there is no intention to create such trust.

In an EFT transaction the payer, who is a customer of the transferring bank, instructs the bank to move funds (credit transfer) from his account to the payee's account. In this case the bank will debit the payer's account, and then the payment is effected,[155] nevertheless, the bank will not hold funds in a separate account for the purpose of transferring it to the payee's account. Accordingly, the view of a separate account does not work in EFT transactions, because it is unlikely that the payer will open a new account to credit it with the

[153] *Re Kayford Ltd (In Liquidation)* [1975] 1 W.L.R. 279 at p. 281 per Megarry J.
[154] *Ibid.*
[155] Cox and Taylor, *Funds Transfers*, *op.cit.,* p. 134

funds issued through a special payment instruction.[156] However, when the customer has more than one account and makes a debit card payment, he should specify which bank account is to be used. Even this, however, does not create a trust fund as long as the account is not uniquely for a single transaction. It is proposed that 'the separation of the money is not the most essential element even in this case, because the two situations, of trust and of the EFT transaction are totally dissimilar.'[157]

The nature of an EFT instruction works against considering it as a trust fund. An EFT instruction to transfer funds from the payer's account to the payee's account can be countermanded, since the EFT system allows this to happen before the final settlement. In contrast, once a payment is considered final, it cannot be revoked. In this sense the payer has possessed the funds up to either the time of implementation of the payment instruction, or the time of payment depending on the EFT system used. The payee in an EFT transaction cannot take any legal action against the paying bank for the funds of the payment instruction, because he has no right to the funds unless the money actually enters his bank account. Conversely, if an EFT order creates a trust fund, the payee could take legal action against the paying bank, as trustee, once the instruction is issued. Ultimately neither the language of an EFT instruction nor its legal nature provide the intention to create a trust fund for the benefit of to the payee; and in the case of there being no clear indication, the jurisdiction is prevented from discovering the effects of such intention.[158]

---

[156] *Ibid.*
[157] Hudson, *op.cit.,* p.284.
[158] *Re Schebsman, Deceased* [1944] Ch. 83.

2.5.3.4 An EFT instruction constitutes a mandate

Within common law,[159] the legal nature of a payment instruction in a credit transfer transaction is regarded as an authority and an instruction from a payer to his bank to transfer a sum of money to a payee's account. This point is illustrated by the decision of Webster J. in *Royal Products v Midland Bank*.[160] The court held:

> "What, then, are the legal implications of those instructions? How are they to be regarded, as a matter of law? In my judgment they are to be regarded simply as an authority and instruction, from a customer to its bank, to transfer an amount standing to the credit of that customer with that bank to the credit of its account with another bank, that other bank being impliedly authorized by the customer to accept that credit by virtue of the fact that the customer has a current account with it, no consent to the receipt of the credit being expected from or required of that other bank, by virtue of the same fact. It is, in other words, a banking operation, of a kind which is often carried out internally, that is to say, within the same bank or between two branches of the same bank and which, at least from the point of view of the customer, is no different in nature or quality when, as in the present case, it is carried out between different banks.".[161]

This decision confirmed that funds transfer is executed by the payer's bank between different accounts in different banks according to the authority conferred by the customer to its bank. Furthermore, the nature of an EFT was scrutinized in the Criminal Division of the Court of Appeal in *R. v King*.[162] Lord Lane held:

> "The CHAPS order is certainly a document. Its effect is to direct the paying bank to debit the paying customer's account with £x (plus any charges) and to transfer the £x to the credit of the payee's account at another bank and to do so by means of an electronic device which would carry out the

[159] *Barclays Bank Plc v Quincecare Ltd* [1992] 4 All E.R. 363; *Libyan Arab Foreign Bank v Bankers' Trust Co* [1988] 1 Lloyd's List Rep. 259.
[160] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 per Webster, J.
[161] *Ibid.*, at p. 198 Webster, J.
[162] *R. v King* [1992] Q. B. 20.

> necessary operations as soon as the staff of the paying bank key the information contained in the document into the machine and then put the machine into operation."[163]

It seems that, within Lord Lane's decision, a payment instruction is a sort of direction or order to the payer's bank, as agent to the payer,[164] to debit the payer's account by the transaction's funds and transfer such funds to the payee's account. That order creates an authority or mandate to make a fund transfer. It does not, however, constitute an assignment of funds. [165] Consequently, the payee's right to the funds transferred issues from the moment of completion of the transfer and not from the moment of delivering the instruction to the payer's bank. The concluded funds transfer constitutes only a mandate and from this two consequences arise: First, the payer has the right to revoke the payment instruction unless it has been executed. Second, the payee has no right to the money transferred until the payment order is completed. [166]

2.6 Conclusion

An EFT is the movement of an amount from a customer's bank account to another's bank account enabling funds to be transferred electronically. Funds transfer operations constitute only a mandate from the customer to the bank to transfer the transactions' funds. The sophistication of EFT has obliged the UK to adopt particular legal frameworks to regulate such transactions. However, this chapter has illustrated that there have been different initiatives in formulating

[163] *Ibid.,* at p.27.
[164] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194; *Libyan Arab Foreign Bank v Bankers Trust Co* [1989] Q.B. 728.
[165] Goode, *Commercial Law*, *op.cit.,* p. 506.
[166] See chapter four, section 4.3.3.

rules to cover EFT transactions. First, there are common law rules. Secondly, there is the CCA 1974 and thirdly, the PSR 2009: these are considered to contain the most significant regulation of EFT transactions. The PSR 2009 are not regarded as final in answering all the legal uncertainties arising in the context of EFT, although they do establish the basic rights, obligations and liabilities of parties involved in EFT transactions.

The remaining chapters of this thesis will investigate the existing rules and principles that could be applied to EFT transactions and their risks. The thesis will show that the rules covering EFT transactions do not ensure certainty and predictability of the parties' rights, obligations and liabilities in the context of EFT transactions. Thus, the previous rules are not adequate and are not capable of being applied to the particular legal problems raised by EFT risks, particularly with regard to the party who bears the risk of non-payment in such transactions. The same inadequacy applies in the context of the liability of the payer and the payer's bank in the case of authenticated but unauthorized EFT orders and, equally important, in the bank's duty of confidentiality against disclosure of customer information in the EFT context. There is also the question of the extent of the bank's liability for direct and indirect damages arising from EFT risks. Under the PSR 2009 the EFT transactions' parties' rights, obligations and liability for unauthorized transaction have been addressed, however the PSR 2009 did not solve the problem of customer identity. Therefore, this thesis argues that the PSR needs to be amended in view of the absence of clarity on the questions of who bears the risk for non-payments; at what point a payment is deemed to be completed; and who bears the risk in cases of authenticated but unauthorized payment instructions.

Chapter Three

EFT Parties' Liability for Unauthorized Payment

3.1 Introduction

EFT users are exposed to various types of unauthorized transactions, for example, fraud, stolen PINs and cards, or misuse of cards.[1] An unauthorized EFT instruction exists when a person who does not have the right to do so initiates a fund transfer instruction. If an EFT instruction issued by a person who does not have the authority to do so accepted then one of the EFT transaction's parties will bear the risk, even if there is no wrongdoing from that party and all reasonable care and skill was taken.[2] The party who bears the risk of this unauthorized payment could be the payer or the payer's bank. The current risk allocation rules are based on the various mechanisms used to access an account and do not create realistic incentives on either the customer or the bank to safeguard against risks in a reasonable manner. The absence of standard legal rules within the EFT system makes it difficult to identify the party that should bear the risk. Thus it is time to regulate the EFT system within one body of law. Although there are laws that specifically address the issues of fraud and other legal problems in the area of internet banking and fund transfers, insufficient attention has been given to remedies. In this era of high-

[1] Shinn, E. T., 'An overview of unauthorised Electronic Funds Transfers: alternatives in reducing consumer liability', (1985) 90 *Commercial Law Journal* 216 at p. 217; Hapgood, M., et al., *Paget's Law of Banking*, (2007), pp. 494-498.
[2] Rusch, L. J., 'Reimagining payment systems: allocation of risk for unauthorised payment inception', (2008) 83 *Chicago-Kent Law Review* 561 at pp. 566-567.

end technology, it is necessary to review and re-examine unauthorized risk processes within EFT transactions. It will be concluded that the present laws are insufficient to address all the uncertainties surrounding unauthorized EFT transactions. This chapter focuses on the allocation of risk in unauthorized EFT instructions. It does so for the following reasons: first, because for some years there has been heated discussion within banking as to who should bear the responsibility in cases of unauthorized EFT transactions. The absence of specific rules devoted to EFT has given rise to an important debate regarding the various parties' rights, obligations and responsibilities in the EFT context, particularly where unauthorized transactions are involved. Secondly, because there is no particular regime governing EFT transactions, problems may arise from the fact that the bank receives the payment instruction from its customer via electronic devices, and in the absence of any physical meeting between the parties the bank may not be able to authenticate the customer's identity and so cannot be certain that the payment instruction is legitimately authorized. PSR 2009, regulation 55, sets out that the payment order will be regarded as authorized when the customer has given consent to carrying out the payment. However, the Regulation does not address the problem of verifying that the payment instruction issued from the rightful card holder. Furthermore, regulation 57 enshrines the customer's obligations in relation to payment transactions, to abide by the terms and conditions regarding use of the card. While regulation 60 places the burden of proof directly onto the bank to show that the unauthorized transaction was authenticated and exactly recorded, and that there was no technical breakdown.[3] Even if the bank shows this, it is not

[3] PSR 2009, regulation 51(3)(a) establishes that when the customer is not business the parties

necessary sufficient to prove that the payment was authorized or that the customer was fraudulent or grossly negligent. Accordingly regulation 61 obliges the payer's bank to refund the transaction funds when the bank made the payment in response to an unauthorized instruction. Nevertheless, the PSR 2009 comes without any indication as to which party bears the losses in case of an authenticated but unauthorized transaction. Finally, there is a problem of security procedures and whether or not a bank has employed an adequate encrypting system to protect its customer data from any attack.

As far as the customers are concerned, the primary basis of liability to the bank will be in contract, and effectively the bank stipulates the terms and conditions. Therefore, the banks do their best to limit and avoid liability in cases of unauthorized EFT transactions. Nevertheless liability could also arise in tort, either for the person who is not customer or for a third party such as a Trusted Third Party. Focussing on an examination of the PSR 2009 and common law principles, this chapter will argue that the existing law inadequate to address the parties' obligations and liabilities for unauthorized payment. Furthermore, applying the law of agency leads to inconsistency and uncertainty in addressing the liabilities of the parties involved in an authenticated but unauthorized instruction.

The outline of this chapter is as follows: section 3.2 will explain the problem of unauthorized EFT instructions. Unauthorized transactions are frequently executed by means of fraud; therefore, the section will contain a clarification of the concept of fraud in commercial civil law. Section 3.3 is devoted to examining

---

may agree that' regulation 60 does not apply.

the existing law, namely agency law and contract law, with regard to the authentication of EFT instructions and the problem of identity authorisation. This section demonstrates that the existing law does not solve the difficulties of either the authentication of customer identity or the bank's liability for authenticated but unauthorized EFT instructions. Thus, it is time to address these problems by determining customers' and banks' liabilities for the authentication of unauthorized transactions in a manner which would be acceptable to both parties. To achieve this aim, section 3.4 will examine the EFT parties' liability for unauthorized EFT instructions. The chapter ends with the conclusion that the existing law does not present a clear and definite account of EFT parties' liability for unauthorized EFT instructions.

3.2 Unauthorized EFT instructions: identifying the problem

There are three different times at which an unauthorized EFT instruction may be initiated. First of all, when the instruction is originally initiated: the best instance of this would be when an authenticated payment instruction is created and transmitted to the payer's bank in the name of a rightful customer but by a person who does not have the right to issue payment order, as in the case of a lost or stolen payment instrument. Secondly, during the transfer procedure of a genuine EFT instruction, as for example when a person who has the authority creates an authenticated payment instruction, but a person who has no authority, such as the payer's bank employee, changes the payment instruction details before the payment instruction is received by the payee's bank. Thirdly, after receipt of the EFT instruction by the payee's bank, for example, when an

authenticated EFT instruction is sent and received in the name of a rightful customer, but some individual, perhaps an employee of the payee's bank, unlawfully changes the payment instruction details before the payment is executed. Unauthorized EFT instructions can in fact happen at any stage of the procedure. However, the most common time for an unauthorized EFT instruction is before or when an instruction is initiated, possibly because this is the most vulnerable point in the EFT procedure. However, any attempt to allocate losses resulting from unauthorized EFT instructions must investigate and provide for all possible cases in which it could happen.[4] This chapter will investigate three different times at which an unauthorized EFT payment instruction may be initiated and the EFT parties' liability for unauthorized transactions in each case.

The most common form of unauthorized EFT transaction is fraud. Fraud, within civil purpose, has been not defined under any statutory provision and thus there is no common definition of fraud.[5] McGrath[6] asserts that deceit[7] constitutes the nearest approximation to a claim in fraud to be found in the English civil law of tort. The test of fraud was laid down in *Derry v Peek*.[8] Stirling J. held that the expression fraud never has been and never will be exhaustively defined,

[4] See Maduegbuna, S. O., 'The effects of electronic banking techniques on the use of paper-based payment mechanism in international trade', (1994) July *Journal of Business Law* 388 at p. 359.
[5] Ulph, J., *Commercial Fraud: Civil Liability, Human Rights, and Money Laundering* (2006), p.6; Kirk, D., Serious Fraud- A Banker's Perspective, in Norton, J., *Banks Fraud and Crime* (1994), pp.1-4; Porter, D., 'Insider fraud: spotting the wolf in sheep's clothing', (2003) 4 *Computer Fraud and Security* 12 at p. 12; McGrath, P., *Commercial Fraud in Civil Practice* (2008), p.3; Goldspink, R., and Cole, J., *International Commercial Fraud* (2004), p. 2; Ormerod, *op.cit.*, p.195.
[6] McGrath, *op.cit*., p.12.
[7] Further about deceit, see Jones, M. A., and Dugdale, A. M., *Clerk and Lindsell On Torts* (2010), Ch. 20; McBride, N., and Bagshaw, B., *Tort Law* (2008), Ch. 23; McGrath, *op.cit.,* Ch. 2; Carty, H., *An Analysis of the Economic Torts* (2001), Ch. 6.
[8] *Derry v Peek* (1889) 14 App. Cas. 337.

because deceit occurs in many and various forms.[9] In *Derry v Peek*, however, Lord Herschell held that in most cases the concept of fraud refers to dishonest misrepresentations. Without proof of fraud, no action of deceit was maintainable.[10] His Lordship defined what must be proved, as follows:

> "Fraud is proved when it is shewn that a false representation has been made knowingly, or without belief in its truth, or recklessly, without caring whether it be true or false. A false statement, made through carelessness and without reasonable ground for believing it to be true, may be evidence of fraud but does not necessarily amount to fraud. Such a statement, if made in the honest belief that it is true, is not fraudulent and does not render the person making it liable to an action of deceit." [11]

According to *Derry v Peek* a misrepresentation can be considered fraudulent only when it is made knowingly, without belief in its truth; or recklessly, heedlessly, without regard to whether it is true or false,[12] although, it is important to comprehend that mere knowledge that the statement made was untrue is inadequate in itself to constitute fraud. Therefore, a person can claim in the tort of deceit only where there is actual fraud.[13] Lord Bramwell stressed the necessities for actual fraud.[14] Lord Bramwell held that:

> "There are various kinds of untruth. There is an absolute untruth, an untruth in itself, that no addition or qualification can make true ... So, as to knowing the truth. A man may know it, and yet it may not be present to his mind at the moment of speaking; or, if the fact is present to his mind, it may not occur to him to be of any use to mention it."[15]

Goldspink and Cole confirm that 'English civil law has never sought to define the expression "Fraud", or to provide a particular rules covering the rights and

---

[9] *Ibid.,* p. 339.
[10] *Ibid.,* at p. 362.
[11] *Ibid.* at p. 337.
[12] The existing law extended accountability for reimbursements to negligent misrepresentation and innocent misrepresentation, see Misrepresentation Act 1967, section 2.
[13] *Derry v Peek* (1889) 14 App. Cas. 337 at p. 346.
[14] *Ibid.*
[15] *Ibid.*, at p. 348.

remedies arising in subject of those whose acting is generally described as fraudulent'.[16] Consequently the rules and remedies governing the civil rights are selected from a variety of legal sources.[17] Kirk's definition could suitably encompass fraud in the environment of commercial civil law:[18] it is "the dishonest non-violent obtaining of some financial advantage or causing of some financial loss".[19] Under criminal law fraud is a combination of two factors: theft and deception.[20] Under civil law, however, theft is treated differently from fraud.[21] Within the Fraud Act 2006, deception is no longer considered a significant element to issue fraud.[22] The Fraud Act 2006 replaced deception offences under sections 15 and 16 of the Theft Act 1968 by stipulate that fraud can be committed in three different methods: by false representation,[23] by failing to reveal information,[24] and by any action which intends to create a gain for him or for another; or cause loss to another or to expose another to a risk of loss.[25] The Fraud Act 2006 states that a representation may be express or implied.[26] Typically, such action would be represented by words or conduct. The Fraud Act 2006 explanatory notes, note 14 illustrates that there is no limitation on the method by which the representation may be expressed; therefore it could be by diverse methods including the spoken or written word.[27] Whether under note 15 a representation falling within the Fraud Act 2006 could be implicit action, such

[16] Goldspink and Cole, *op. cit.,* p. 12.
[17] *Ibid.*
[18] Ulph, *op.cit.,* p. 6; Kirk, *op.cit*., pp. 1-4.
[19] Kirk, *op.cit*., p. 11; Further, see Haynes, A., 'Market abuse, fraud and misleading communications', (2012) 19 (3) *Journal of Financial Crime* 234 at p. 240.
[20] Leigh, H. L., Banks-Fraud and Crime: A Survey of Criminal Offences under English Law*,* in Norton, J., (ed), *Banks Fraud and Crime*, (1994), pp.1-4.
[21] Ulph, *op.cit*., Ch. 11.
[22] The Fraud Act 2006, Chapter 35, section 1.
[23] *Ibid.,* section 2.
[24] *Ibid.*, section 3.
[25] *Ibid.*, section 4.
[26] *Ibid.*, section 2(4).
[27] Fraud Act 2006, Explanatory Notes, note 14.

as an invalid holder using the rightful holder's card dishonestly and without authority.[28] The Act created a new goal, that of bringing within the ambit of criminal law the latest methods of communication technology used to process internet transactions.[29] Hence, section 2(5) specifies cases where false representation applies to the latest methods of communication technology, for example chip and PIN.[30] Accordingly, in the context of EFT transactions a fraudulent action falls under the Fraud Act 2006, as an EFT instruction by electronic device involves either the transfer or receipt of funds.[31] Ormerod argues that there is adequate protection against electronic fraud within section 2 of the Fraud Act 2006.[32]

Furthermore, subject to the offence of conspiracy of defraud the common definition of a conspiracy of defraud was presented in *Scott v Metropolitan Police Commissioner*[33] by Lord Dilhorne when he held that:

> "an agreement by two or more by dishonesty to deprive a person of something which is his or to which he is or would be entitled and an agreement by two or more by dishonesty to injure some proprietary right of his, suffices to constitute the offence of conspiracy to defraud."[34]

Conspiracy to defraud then has two elements; dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled, and second element is to injure some proprietary right. This does not require the

[28] *Ibid.,* notes 15.
[29] Ormerod, D., 'The Fraud Act 2006 - criminalising lying', (2007) *Criminology law review* 193 at p.195.
[30] Fraud Act 2006, Explanatory Notes, note 17.
[31] Haynes, *op.cit.,* p.241.
[32] Ormerod, *op.cit.,* p.200; Also, see Ahmad, N., 'E-Commerce and legal issues surrounding credit cards: emerging issues and implications', (2009) 15 *Computer and Telecommunications Law Review* 114 at p. 120.
[33] *Scott v Commissioner of Police of the Metropolis* [1975] A.C. 819.
[34] *Scott v Commissioner of Police of the Metropolis* [1975] A.C. 819 at p. 840.

defendants' actions to directly result in the fraud. In *R v Hollinshead*,[35] the House of Lords held that creating devices designed to alter electricity meter readings constituted conspiracy to defraud, even though the actual fraud would be executed by members of the public rather than the conspirators. In these positions, it is not necessary for the actions to lead directly to loss for the injury party; these are when the conspirators plan to deceive a person holding public office into acting counter to their duties, and when the conspirators know that their actions put the injury party's property at risk, even if the risk never materialises.[36]

Furthermore, subject to the offence of conspiracy of defraud, section 1(1) of Criminal Law Act 1977 states that:

> "… if a person agrees with any other person or persons that a of course of conduct shall be pursued which will necessarily amount to or involve the commission of any offence or offences by one or more of the parties to the agreement if the agreement is carried out in accordance with their intentions, he is guilty of conspiracy to commit the offence or offences in question.

This section does not affect the common law offence of conspiracy so far as it relates to conspiracy to defraud. Although, in *Wai Yu-Tsang v R*[37] a conspiracy to defraud is 'not limited to the idea of economic loss, nor the idea of depriving someone of something of value. It extends generally to the purpose of fraud and deceit... if anyone… be prejudiced in any way… that is enough'.[38] In this regard, it is not necessary for the crime to be completed, only some part of it, deception

[35] *R. v Hollinshead* [1985] A.C. 975.
[36] Herring, J., *Criminal Law* (2008), p. 811.
[37] *Wai Yu-Tsang v R* (1991) 1 WLR 1006.
[38] *Ibid.*

is not a necessary element because 'the crime is complete where the intention is to cause the victim economic loss by dishonest means'.[39]

In the EFT context, fraud means an unauthorized payment instruction which happens whenever the payment instruction is unlawfully created or changed by a person who has no right to do so in order to debit the payer's account. Generally, fraud in the context of EFT can occur in two ways, either offline or online.[40] Transactions such as those when the fraudulent person is face to face with the seller are known as offline fraud because they do not involve the use of the internet. Online fraud by definition occurs via the internet.[41] In the case of offline purchases, the payee (seller) should be able to verify the payer's identity since the transaction takes place with the payer face to face, while, in online transactions such verification, even with the use of security procedures is not easy and may be impossible. Consequently, the fraudster has an opportunity to use an unauthorized instrument with the rightful holder's information in order to make transactions. Methods of perpetrating fraud have become more diverse as technology has become more sophisticated. As a result, banks choose from a variety of security procedures and rules to protect against the risk of fraud or forgery and these are included in the terms and conditions of the agreement between the bank and the customer.[42]

[39] *Scott v Commissioner of Police of the Metropolis* [1975] A.C. 819 at p. 822.
[40] Ahmad, *op.cit.,* p. 116; Akintoye, K. A., and Araoye, O. I., 'Combating e-fraud on electronic payment system', (2011) 25 *International Journal of Computer Applications* 48 at p. 48.
[41] David, S.W.*, Cybercrime, the Information of Crime in the Information Age* (2007), Ch.5.
[42] See section 3.3.2.

3.3 The basic schemes: authentication of EFT instructions

An authority can be divided into two types, actual and apparent. Actual authority may be explicit or implicit.[43] It is explicit when the principal, the customer, expressly confers upon the agent, the bank, an authority to do something for and on behalf of him. Implicit authority is when it is inferred from the parties' words and conduct that the agent has such power.[44] While, apparent or ostensible authority arises where a customer (the principal) deliberately or through want of ordinary care causes or allows a third person to believe that he is bound by the acts of another person (the agent).[45] The principal only creates an inference that an agent has authority to act on his behalf even though no authority exists in fact.[46] This is well illustrated by Lord Denning M.R. in *Hely-Hutchinson v Brayhead Ltd:*[47]

> "It is there shown that actual authority may be express or implied. It is *express* when it is given by express words, such as when boards of directors pass a resolution which authorises two of their number to sign cheques. It is *implied* when it is inferred from the conduct of the parties and the circumstances of the case, such as when the board of directors appoints one of their number to be managing director. They thereby impliedly authorise him to do all such things as fall within the usual scope of that office…. Ostensible or apparent authority is the authority of an agent as it *appears* to others."[48]

Actual or apparent authority of an agent governed by agency law and this governance is of essential importance in the context of unauthorized EFTs because the norms of agency law apply to determine whether or not an EFT

[43] Beatson, J., et al., *Anson's Law of Contract* (2010), p. 687.
[44] *Ibid.*
[45] Reynolds, B., *Boustead and Reynolds on Agency* (2001), p. 90 and p. 307; Markesinis, B. S., and Munday, R. J. C., *An Outline of the Law of Agency* (2005), pp. 36-37.
[46] Beatson, *op. cit.,* pp. 687-688.
[47] *Hely-Hutchinson v Brayhead Ltd* [1968] 1 Q.B. 549.
[48] *Ibid.,* at p. 583.

instruction is authorized. However, the application of the norms of agency law raises the issue of identity authentication and also the issue of whether the EFT instruction is an authorized one.[49]

3.3.1 The existing law to authenticate EFT instruction and the problem of identity authorization

The PSR 2009 rules that an authorization of payment instruction must be used in accordance with the personalised security features of the payment instrument agreed between the parties,[50] for example, chip and PIN. Existing law deals with authorization solely in the context of the payer's express approval,[51] which is clearly compulsory. Such approval may be given before the bank executes the instruction, or after the execution of the payment instruction if this is agreed between the parties.[52] Such approval must be given 'in the form, and in accordance with, the procedure agreed between the payer and the bank'.[53] Only express approval is dealt with here and the law seems quite unhelpful in defining situations where the customer might be taken implicitly to have authorized a transaction. Thus, there should be clarification of the point at which the law accepts implicit approval for the execution of EFT instructions, for example, a cardholder voluntarily gave the card and the security procedures to a friend or relative. Geva argues that: 'The reference to an agreement, as well

[49] Hapgood, et al., *op.cit*., p.336.
[50] PSR 2009, regulations 57(1)(a). Payment instrument is defined under regulation 2(1) as: "any (a) personalised devices; or (b) personalised set of procedures agreed between the payment services user and the payment service provider, used by the payment service user in order to initiate a payment order".
[51] PSR 2009, regulation 55(1).
[52] *Ibid,* regulation 55(2)(a).
[53] *Ibid,* regulation 55(2)(b).

as a procedure, weakens the possibility of an implied authority and may be read to eliminate altogether the possibility of an apparent authority'.[54]

Another flaw that may be held against regulation 55 of the PSR 2009 is that there is nothing to indicate that the payee's authorization has been given to his bank for executing a debit transfer from the payer's account. Thus, the norms of agency common law need to be applied to determine whether or not the EFT instruction is an authorized one.

It is argued[55] that the legal nature of funds transfer is only a mandate passed from the customer to the bank to transfer or collect the transaction funds. Thereby, the general rules of agency law apply to EFT transitions and, banks act as agents to their customers, and thus the banks are bound to execute their customers' mandate.[56] The mandate is an authority from the customer to his bank.[57] Thus as long as the bank has the customer's authority to pay a cheque, it is entitled to debt the customer's account.[58] Geva stated that in EFT transactions, an unauthorized instruction 'must initiated from someone who either presumed control of the access device illegally, or bypassed the access device altogether. Such a person may be one of the customer's member family, the customer's employee or associate, or a total stranger'.[59] In contrary, an authorized EFT instruction is a mandate created the customer or by a person

[54] Geva, B., 'Payment transactions under the EU Payment Services Directive: a U.S. comparative perspective', (2009) 27 *Penn State International Law Review* 713 at p. 725.
[55] Hudson, P., and Mann, J. E., *Commercial Banking Law* (1978), p. 283; Arora , *Electronic Banking and the Law, op.cit.,* p. 21; Chitty, J. D., *Chitty on Contracts* (2008), para. 5954; Cox, R. and Taylor, J., 'Funds Transfers', in Brindle, M. and Cox, R., *Law of Bank Payments* (2010), p. 128; Ellinger, E., et al., *Modern Banking Law* (2011), p. 593.
[56] See chapter two, section 2.5.1.1.
[57] *Fielding v Royal Bank of Scotland Plc* [2004] WL 62144 at para. 56.
[58] *Ibid.*
[59] Geva, B., *Banking Collections and Payment Transactions* (2001), p. 394.

authorized by the customer to issue a payment instruction. The authority of an EFT instruction can only be examined with regard to procedures agreed between the customer and the bank.[60] Accordingly, the bank has no right to debit its customer's account due to an unauthorized EFT instruction or outside the limitation of the customer mandate.[61]

Given the above position, it seems that applying the rules of mandate does not give the bank the required protection. Therefore, the bank will be reluctant to carry out the payment instruction entirely or may choose not to carry out it at high speed or at a low cost. The reason for such reluctance is that due to the electronic access to issue EFT instruction it is difficult for the bank to determine its customer's identity or to verify that the person who issues the instruction is the customer himself or someone entitled by the customer's actual or apparent authority. Therefore, the significant issue in identity authentication is that of identifying the person who passed the mandate and ensuring that he is authorized to do so. If the bank is assured of that identity it will be free from the responsibility for a forged or unauthorized payment instruction. There is therefore an important relationship between the mandate and identity authentication in settling payments. If the bank debits a customer's account with settlement of a cheque that he did not sign, the bank has no right to such a debit and has to credit its customer's account with the money charged.[62] The author's view is that applying the agency law rules to EFT leads to the conclusion that authenticated EFT instruction is authorized only when issued by

[60] Robertson, et al., 'Internet Payments' in Brindle, M., and Cox, R., *Law of Bank Payments* (2010), p. 328.
[61] Arora , *Electronic Banking and the Law, op.cit.,* p. 135; Hapgood, et al., *op.cit*., p.336.
[62] *Greenwood v Martins Bank Ltd* [1933] A.C. 51; *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] A.C. 80; *Patel v Standard Chartered Bank* [2001] Lloyd's Rep. Bank. 229.

a person who has the authority to do so. Consequently, an authenticated EFT instruction initiated by a person who has no authority to do so is an unauthorized instruction, and the bank has no right to debit its customer's account. Taking into consideration that a bank has the right to debit its customer's account when the customer has given his implied authority to another person such as a friend or relative to withdraw funds from his account. Thus, if the unauthorized transaction takes place due to the implied authority the bank bears no liability to its customer. Furthermore, when the customer acted fraudulently or negligence the bank bears no liability to the customer. Therefore, within agency law the payer's bank's liability for authenticated but unauthorized payment instruction is unclear and unpredictable.

Eventually, however, an unauthorized EFT came to be viewed as analogous to a forged or unauthorized cheque.[63] Pennington reasoned that if a bank debits its customer's account in accordance with an unauthorized payment instruction, the legal consequences would be as if the bank had honoured a forged or unauthorized cheque.[64] The legal position of a bank in the case of a forged and unauthorized cheque is described in section 24 of the Bills of Exchange Act 1882 which states:

> "Subject to the provisions of this Act, where a signature on a bill is forged or placed thereon without the authority of the person whose signature it purports to be, the forged or unauthorised signature is wholly inoperative, and no right to retain the bill or to give a discharge therefore or to enforce payment thereof against any party thereto can be acquired through or under that signature, unless the party against whom it is sought to retain or enforce payment of the bill is precluded from setting up the forgery or want of authority.

[63] Pennington, R., 'Fraud, Error and System Malfunction' in Goode, R., *Electronic Banking*: *The Legal Implications* (1985), p. 70.
[64] *Ibid.*

> Provided that nothing in this section shall affect the ratification of an unauthorised signature not amounting to a forgery."

This section explicitly confirms that the holder of a bill with a forged or unauthorized signature has absolutely no rights against the bank. Furthermore, in the case of a forged cheque paid by the bank, the inference is that the bank is acting without its customer's mandate and is not authorized to debit the customer's account.[65] Accordingly, the bank is liable to the customer if it makes a payment outside the limits of his mandate, and the customer may sue it for damages.[66] In view of this, in the context of EFT transactions, if the bank debits its customer's account according to an unauthorized instruction it is the bank's responsibility to re-credit the customer account with the funds that had been debited due to the unauthorized instruction.[67] Regards to EFT, it is not reasonable to draw an analogy between the rules applicable to an unauthorized cheque and those which apply to electronic payment; that it is because EFT systems involve different technology issues, to which the application of the current law will not bring resolution of the problems. For example, EFT by any electronic device must be authenticated by using electronic security procedures. This raises the issue of identity authentication and in the context of EFT the situation is not comparable with that of an unauthorized cheque. Smart[68] argues such point by states: 'the optimist may suggest that there is nothing basically new in EFT; it is only a new method of charge. Therefore, any legal issue could be solved by analogy with existing law. Certainly the cheque, which binds the

[65] Greenwood Hapgood, et al., *op.cit*., p. 336; Arora, *Electronic Banking and the Law*, *op.cit.,* p. 135.
[66] Arora, *Electronic Banking and the Law, op.cit.,* pp. 135-136.
[67] Cox and Taylor, *op. cit.,* p. 186.
[68] Smart, E., 'Electronic Banking: An Overview of the Legal Implications', in Goode, R., *Electronic Banking*: *The Legal Implications* (1985), p. 1.

bank only when it agrees to pay the cheque and which presents the unpaid payee with a right of action against the payer, is an uncertain basis for analogy'.[69] Furthermore, Geva argues that the bank's duty to disclose and prevent unauthorized EFT payments depend on the security procedures used, thus it differs from a method to another.[70] Geva has also elucidated that in the case of a forged manual signature the bank is obliged to verify and detect the manual signature on each cheque to ensure that the cheque is authenticated.[71] By contrast, in an EFT the bank is obliged to examine the instruction by means of its automated security procedure.[72] It is arguable that the hand-written individual signature determines the person who has signed the cheque,[73] whereas the electronic security procedures for authenticating the payment instruction do not identify the person who issues that instruction.[74] Therefore, the existing law does not solve issues relating to unauthorized EFT transaction, particular the issue of an authenticated but unauthorized EFT instruction. Thus, any an analogy results in unpredictability and lack of clarity with regard to the parties' liabilities in cases involving authenticated but unauthorized EFT.

Generally speaking, the customer's instruction is binding upon him as its lawful issuer if it was initiated by him or with his express or implied authority and the bank which has executed its customer's EFT instruction after it has passed the test of rightful authentication is allowed to pass the payment by debiting the

[69] *Ibid.*
[70] Geva, *Bank Collections and Payment Transactions* (2001), p. 395.
[71] *Ibid.*
[72] *Ibid.*
[73] Hapgood, et al., *op.cit.,* p. 407.
[74] *Ibid.*

customer account.[75] Furthermore, if the customer acted fraudulently the bank has the right to debit its customer's account. In this context, it is important to examine whether authentication by means of various "security procedures" is regulated by particular legislation dealing with the authentication of EFT instructions in ways similar to that of mutual signature. To examine this issue, the different forms of authentication procedure need to be explained separately and in detail in order for it to be decided whether the law recognises them as means of authentication. Accordingly, the next sections will examine the types of authentication procedure, such as passwords, user names, digital signatures and Trusted Third Parties (TTP), to ascertain whether they have legitimacy in English law. The legal aspects of authentication procedures will be examined in order to discover the extent to which they affect EFT parties in cases of authenticated but unauthorized EFT instruction. The following sections will express the conclusion that the authentication procedures under English law have legal legitimacy as evidence. Authentication is nevertheless defined with reference to the ability of the bank to use any security procedure to verify the authorization by means of a payment device.[76] It is the customer's duty to inform his bank 'without undue delay' upon becoming aware of the unauthorized payment. However, the delay can never exceed 13 months from the date when the payer's account was debited with the payment.[77] Although, in the case of business customers the parties (bank-customer) may agree that a different time period applies.[78] However, it is the bank's duty to prove that the payment

[75] Davies, B., 'What is the extent of the customer's duty not to facilitate fraud?', (2009) 30 (11) *Business Law Review* 238 at p. 241.
[76] PSR 2009, regulation 60(2).
[77] *Ibid.,* regulation 59(1).
[78] *Ibid.,* regulation 51(3)(a).

instruction was authenticated in cases where the customer denies authenticating the payment instruction. [79] If the bank reports that the authentication used the lawful security procedure, this is not in itself necessarily sufficient to indicate or prove the payment was authorized by the lawful customer.[80] Therefore, except when the payer's bank proves that the payer authorized the payment order, it should refund the amount of the payment. The legal validity of authentication procedures and their consequence for the EFT parties in cases of authenticated but not authorized EFT instruction is not regulated by specific legal norms and such absence leaves the parties with the right to regulate their agreement. This absence also allows the banks to protect themselves by establishing terms by which they bear no liability for authenticated but unauthorized EFT instructions carried out by a third party.

3.3.2 Authentication procedures: functions, forms and validity

One method of authentication in paper based settlement transactions is the signature. Guest[81] defined a signature in this context as; 'the writing of a person by his hand on a receipt or piece of paper to authenticate the payment order transaction'. With regard to EFT transactions, authentication methods have been changed by the use of electronic keys.[82] The customer uses a user name

[79] *Ibid.,* regulation 60. Although, where the customer is not consumer the parties (bank-customer) may agree that regulation 60 does not apply, regulation 51 (3)(a).
[80] *Ibid.,* regulation 60(3).
[81] Guest, A. G., *Chalmers and Guest on Bills of Exchange, Cheques and Promissory Notes* (2009), p. 249.
[82] *Report by the Review Committee on Banking Services: Law and Practice*, ("The Jack Report") (1989, London, HMSO, Cm 622), p. 77.

and password to execute the electronic mandate and transmit it to his bank.[83] Initiating the payment order in correct user name and password means the payment order is authenticated, and received by the customer's bank via an electronic access key, irrespective of whether the person who issues the instruction is authorized to do so or not. Authenticating the payment order is done by security procedures employed by the bank.[84] In practice banks employ different types of security procedure, for example, passwords, user names, electronic signatures and TTP, all of which will be examined in this section.

On-line transactions raise difficulties for banks: they need to ascertain the identity of their customers and to ensure that the person who sends the mandate is entitled to do so by the customer himself or his actual or apparent authority. Therefore the verification of personal identity is of the greatest importance. Once the identity of the customer is authenticated the bank will no longer be responsible in cases of forged or unauthorized payment order. The functions of the authentication procedure are: firstly, to ensure the identity of the customer who issued the payment instruction;[85] secondly, to ensure that customer data are not accessible to persons other than the rightful holder; and thirdly, to use the security procedure agreed between the bank and customer as a non-repudiation measure, preventing the customer from denying the execution of the instruction.[86]

[83] Arora, *Electronic Banking and the Law, op. cit*., pp. 128-129.
[84] Azzouni, A., 'Internet banking and the law: a critical examination of the legal controls over internet banking in the UK and their ability to frame, regulate and secure banking on the net', (2003) 18 *International Banking Law and Regulation* 351 at p. 355.
[85] PSR 2009, regulation 58(1)(a).
[86] Robertson, et al., *op.cit*., p. 328.

Before clarifying the different forms of authentication procedures involved with on-line EFT, it would be appropriate to start with the general meaning of encryption technique. Encryption technique is defined as: “the process of using an algorithm, a mathematical rule, to translate a given message into a jumbled form which is then unreadable by anyone who does not have the correct mathematical rule to translate the message back into its original form.”[87] An encryption technique exists in two different forms: a symmetrical key and public key encryption. With a symmetrical key code the data is encrypted and broken with the same key.[88] The deliverer encrypts the data before delivering it to the receiver and thus the data becomes unreadable. The key that encrypted the data must also be used for the decryption in order for the data to be readable. The receiver who wants to break through this data must have the same key. The best instance of the symmetrical key using is between banks in the SWIFT system. Robertson et al.[89] argue that the best environment for a symmetrical encryption key is one where the number of users is relatively limited and where users can rely on each other to keep the shared key secure. Nevertheless, the data is coded and broken with the same key, which makes the symmetrical encryption key more vulnerable to being hacked and revealed.[90] For that reason a new encryption system, known as public key encryption, has been established.

The function of public key encryption is to protect customers’ data and solve the problem involved in the use of the symmetrical key. Public key encryption

[87] *Ibid.,* at p. 329.
[88] *Ibid*.
[89] *Ibid.*
[90] *Ibid.*

requires a pair of keys; two uniquely related cryptographic keys, one public and one private.[91] The public key is made available to everyone via a publicly accessible repository or directory. The use of the private key, however, must be restricted to its owner. The purpose of the private key is to encrypt data which is known to the owner alone, whereas the purpose of the public key is to decrypt data which is known to the bank.[92] Public key encryption works as follows: the customer who keeps the private key can sign the payment instruction and encrypt the data with the private key and send it to the bank, which can decrypt the data with the public key.[93] Where the public key can decrypt the data, the data is verified and sent to the customer, who has the private key. Normally the private key (chip) is saved on the customer's smart card. The customer allows access to the private key by entering a password or PIN.[94] Public key encryption is considered more difficult and less vulnerable to attack than the symmetrical encryption key because different keys are used to encrypt and decrypt the same data.[95]

Azzouni has elucidated the legal problems related to internet banking, for instance fraud, forgery and security procedures. Moreover, the responsibility of the parties in an EFT has been left unresolved.[96] He has correctly argued that the reason for this unsatisfactory situation is that when the current laws

[91] See https://www2.swift.com/search/redirect.faces 15 March 2013.
[92] Kelman, A., 'An Introduction to Electronic Payment Mechanisms, Encryption, Digital Signatures and Electronic Surveillance', in Chissisck, M., and Kelman, A., *Electronic Commerce, Law and Practice* (2002), p. 175.
[93] Spyrelli, C., 'Electronic signatures: a transatlantic bridge? An EU and US legal approach towards electronic authentication', (2002) 2 *Journal of Information, Law and Technology* http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html 23 February 2011.
[94] Angel, J., 'Why use digital signatures for electronic commerce?', (1999) 2 *Journal of Information, Law and Technology* http://elj.warwick.ac.uk/jilt/99-2/angel.html 23 February 2011.
[95] Robertson, et al., *op.cit*., p. 330.
[96] Azzouni, *op.cit*., p. 351; Geva, Consumer liability in unauthorised Electronic Funds Transfers', (2003) 38 *Canadian Business Law Journal* 207 at p.224.

regarding special contracts, agency, and forged cheques are applied to internet banking there is ambiguity and uncertainty with regard to liability in cases of unauthorized transaction orders. [97] Azzouni explained the situation as follows:

> "The discussion of the different types of services, security, privacy and other legal issues, reveals that there are still many uncertainties regarding most aspects of online banking. The diversity in interpreting legal provisions and the different decisions held in cases with identical facts is another example of the incapability of the traditional law to lead with the distinct nature of the internet. Furthermore, in the absence of regulations dealing with specific issues of internet banking, such as liability, banks draw these rules trying to achieve the minimum liability in cases of system malfunctions and fraudulent transactions. Additionally, the diversity of rules between the different countries is an obstacle to the development of internet banking."[98]

Within the PSR 2009, authentication has been defined by reference to the type of payment instrument and the methods employed for the verification of its use.[99] However, PSR fails to determine and resolve the problem of identity authentication. Differing solutions to the problems of security procedures have been suggested. The standard forms of security procedure for authenticating the EFT instruction and verifying the customer's identity are chip and PIN, although there is nothing to prevent the EFT transaction parties from agreeing to other methods, for example, electronic signatures or TTP.

Passwords and user names as a security procedure in electronic payments are common to all banks due to their low cost and ease of use.[100] However, regarding passwords and user names in machines there are two weaknesses:

---

[97] Azzouni, *op.cit*., p. 362.
[98] *Ibid.*
[99] Regulation 60(2): "authenticated means the use of any procedure by which a payment service provider is able to verify the use of a specific payment instrument, including its personalized security features.".
[100] Azzouni, *op.cit.,* p. 354; Geva, Consumer liability in unauthorised Electronic Funds Transfers, *op.cit.,* p. 224.

first, they are issued only for existing authentication[101] and secondly, they are insecure.[102] Passwords as a security procedure are therefore always combined with a form of identity authentication or with a payment transaction authentication.[103] Banks are encouraged by the UKPA to use multi-factor authentication security in internet banking.[104] Thus, since 2006 multi-factor authentication security has become standard in banks. Standard multi-factor authentication security in internet banking will comprise a small instrument namely, a PIN and device.[105] At the beginning of 2013 the Payment Council[106] announced that if a customer has difficulties in printing a PIN, he or she has the right to request from the bank to use the multi-factor authentication security method in internet banking, the chip and signature card. The multi-factor authentication of security, namely chip and signature cards, can be used by a person who has dexterity issues, visual impairment, memory problems or mobility issues which make it hard to use a PIN terminal.[107] Using multi-authentication security devices does not represent a final solution to the problem of unauthorized transactions, although it makes unauthorized instructions more difficult.

---

[101] Jiang, S., and Gong, G., 'Password based key exchange with mutual authentication', (2005) 3357 *Lecture Notes in Computer Science* 267 at p. 270.
[102] Ford, M. D., 'Identity authentication and e-commerce', (1998) 3 *Journal of Information, Law and Technology* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/ford 23 February 2011; Liao E., et al., 'A password authentication scheme over insecure network', (2006) 72 *Journal of Computer and System Sciences* 727 at p.727.
[103] Joris, C., et al., 'On the security of today's on-line electronic banking systems', (2002) 11 http://www.linkedin.com/in/jorisc/pub/stoebs.pdf 21 February 2013.
[104] UKPA, Payment Council, *Multi-factor Authentication Security Review*, 2012 http://www.paymentscouncil.org.uk/resources_and_publications/publications/fraud_publications/-/page/2415/ 12 February 2013.
[105] UKPA, Payment Council, *PIN entry device protection profile common criteria evaluation* http://www.theukcardsassociation.org.uk/technical_services_standards/pin_entry_device_protection_profile.asp 12 February 2013.
[106] UKPA, Payment Council, *Improving awareness of the alternative for people who are unable to use a PIN,* 2013 http://www.paymentscouncil.org.uk/current_projects/chip_and_signature/ 12 February 2013.
[107] *Ibid.*

Passwords and user names are methods for authenticating payment instructions. However, the weaknesses in these methods and the sophistication of electronic banking through funds transfer systems causes the banks to be always in search of new security methods equal to the latest technological developments.[108] Accordingly, the electronic signature[109] and the TTP have emerged as security procedures for verifying the identity of the customer and also as means of authenticating payment instructions.

3.3.2.1. Electronic signature

An electronic signature (e-signature hereafter) is defined by the UNCITRAL Model Law on Electronic Signatures 2001 as: 'data in an electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of information contained in the data message.'[110]

The UNCITRAL Model Law on Electronic Signatures assumes that if the signature issues data it is uniquely connected to the customer. E-signatures are defined by Spyrelli as "computer-based personal identities".[111] There are various ways to exercise an e-signature, such as an electronic sound, (a person's voice), a symbol, (a pictorial representation of a person in a JPEG file) and a process, (a procedure that conveys assent), attached to or logically

[108] Angel, *op. cit*.
[109] The Electronic Communications Act 2000 chapter 7.
[110] UNCITRAL Model Law on Electronic Signature (2001), article 2(a).
[111] Spyrelli, C., 'Electronic signatures: A transatlantic bridge? An EU and US legal approach towards electronic authentication', (2002) 2 *Journal of Information, Law and Technology* http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html 23 February 2011.

associated with a record.[112] Any of these forms could be adopted by a customer with the intention to sign the record. An e-signature is not difficult to execute as long as something as easy as a typed name can serve as one.[113] Digital signature[114] is considered to be the most common form of e-signature.[115] Mason and Bromby[116] argue that an e-signature is a generic term which refers to all methods of e-signature, such as the PIN, the words 'I accept', and the writing of the personal name in an email. Digital signatures have three functions: first, to authenticate the payment instruction by identifying the person who issued the instruction; secondly, to protect the customer's data from any attack; and thirdly, to prove that the transaction is authorized by the lawful person.[117] Angel has elucidated these functions, as follows:

> "1. Authentication – to authenticate the identity of the person who signed the data so it is known who participated in the transaction.
>
> 2. Integrity – to protect the integrity of the data so it is possible to know the message read has not been change, either accidentally or maliciously.
>
> 3. Non-repudiation, to allow it to be proved later who participated in a transaction so that it cannot be denied who sent or received the data."[118]

A digital signature is like a 'classical paper-based signing' but it is one 'which takes the concept of a personal signer and turns it into an electronic device.[119] It exists in two forms: the symmetrical key and public key encryption,[120] which is

---

[112] Spyrelli, *op.cit*.; Mason, S., and Bromby, M., 'Response to digital agenda for Europe: electronic identification, authentication and signatures in the European digital single market: public consultation', (2012) 3 *European Journal of Law and Technology* 1 at p. 2; Wang, M., 'Do the regulations on electronic signatures facilitate international electronic commerce? A critical review', (2007) 23 *Computer Law & Security Report* 32 at p. 32.
[113] Spyrelli, *op.cit*.
[114] Further details about the difference between e-signature and digital signature, see Mason, S., *Electronic Signatures in Law* (2003), pp. 99-101.
[115] Spyrelli, *op.cit.;* Mason, and Bromby, *op.cit*., p. 2.
[116] *Ibid.*
[117] Angel, *op.cit.*
[118] *Ibid.*
[119] Robertson, et al., *op.cit.*, p. 340.
[120] Wang, *op.cit.,* p. 32.

based on an encryption technique.[121] As explained above, with a symmetrical key the data is encrypted and broken with the same key. The electronic device is private to both the document and the signer and binds both of them together.[122] Digital signatures ascertain the authenticity of the signer. Thus, any alteration made to the document after it is signed means an unauthorized person has altered the signature. Digital signatures moreover protect against illegal signatures and information changes.[123] More recently, SWIFT establishes a multi-bank personal digital identity solution known as 3SKey. The solution, usable on the SWIFT network but also on proprietary networks or the internet, allows corporate user to sign financial messages and files sent to their banks, using a single signing device. It also offers banks a cost-effective way to implement secure authentication in electronic banking services by using a shared, reliable and trusted public key infrastructure, which guarantees to both banks and customers that their transactions are authentic, unchanged and legally binding. 3SKey digital signatures ensure that the data is coming from the attributed corporate user, that the content has not been changed after the approval process and presents a proof of signature.[124]

Nonetheless, whichever method is employed an e-signature is insufficient to solve the problem of identification.[125] This can be demonstrated by asking the question: how can a bank be certain that the security procedures used by the person belong to the person who has the authority to make EFT transaction, since the security procedure has no intimate relationship with any one. The

[121] Angel, *op.cit.*
[122] *Ibid.*
[123] Robertson, et al., *op.cit.*, p. 333.
[124] http://www.swift.com/products/3skey 19 March 2013.
[125] Robertson, et al., *op.cit.*, p. 333; Spyrelli, *op.cit.*

answer is that there is no guarantee that the security procedure emanates from the person who has the authority to do so. These types of security procedures do not solve all the problems relating to unauthorized EFT instructions. It appears then, that an e-signature is not the solution with regard to maintaining tight security, as there is nothing to prevent a person from typing another person's name. Therefore, this solution does not represent an advance in security and is to be considered an insecure way of signing documentation. In addition, it is not the best method for preventing unauthorized transactions because it cannot reliably prove any connection between the e-signature and the person who has the authority to prove the customer's identity. Moreover, Robertson et al [126] consider that an e-signature does not fill the gap when a third party in some legal cases needs to decrypt the security device and access encrypted data, such as in cases involving the prevention of money laundering.

A number of legal authors[127] have argued that the Trusted Third Party (TTP), or alternatively the Certification Authorities (CA), is the best method to amend this shortcoming and ensure that the security procedure belongs to the authorized person. However, Robertson et al note that 'the British Government has refused the option of imposing mandatory deposit of private keys because of concerns about the civil liberty implications'.[128] Nevertheless, the TTP could be used by a bank on a voluntary basis. The question which remains, however, is whether the TTP can fill the security gap and help to determine the identity of the person who uses the security procedures to send the payment instruction.

[126] Robertson, et al., *op.cit.*, p. 335.
[127] *Ibid.*, at p. 334; Spyrelli, *op.cit.*; Wang, *op.cit*., pp. 32-33.
[128] Robertson, et al., *op.cit.*, p. 335.

3.3.2.2 The Trusted Third Party

TTP acts as a depositary for both public and private encryption keys. For instance, where a first participant uses his or her private key to link with another participant while not knowing the public key, the first participant can request that key from a TTP. Also, in cases of a private key, a legal user can request such a key from the TTP, for example in case of the death of the owner. There is a similarity between the operation of the TTP and a notary in civil law jurisdictions.[129] The notary has to guarantee that a particular user has signed a document, after ensuring his or her identity by comparing the information with some other form of official identity, such as a passport.[130] Instead of depending on the e-signature to check a person's identity, the TTP has the right to request from the person another form of security procedure to ensure a user's identity. For example, the TTP may ask the user to bring a certificate which is an attestation from the notary guaranteeing the authenticity of the personal details provided. Relying on this certificate, the TTP issues an electronic certificate confirming that a specific firm owns particular public and private keys.[131] Such electronic certification is authenticated by the TTP to authorize the use of a private key.[132] The bank supplying the EFT service could be the TTP which issued the certificate and the certificate of authority is presented to ensure that the digital signature belongs to the rightful holder.

[129] *Ibid.*, p. 336.
[130] Angel, *op.cit.*
[131] Robertson, et al., *op.cit*., p. 336.
[132] Angel, *op.cit.*

Indisputably, the user passes a payment instruction to the bank in the form of a: a digital signature and the certificate transferred to the bank. Before passing the payment instruction, the TTP will check the digital signature and the certificate to guarantee that such an instruction has been executed by the rightful person.[133] Even so, such use does not prove that the lawful person issued the instruction. The user's private key is an electronic file which could be used and copied by hackers on the internet. It seems that the TTP is not the best solution to fill the security gap regarding a customer's identity. This being the case, the question of which party will bear the losses in cases of authentication of an unauthorized EFT instruction remains unanswered. Since the common law of contract applies to the EFT relationship between the bank and the customer in the context of unauthorized EFT, banks in their agreements avoid liability for authenticated but unauthorized payment instructions in explicit conditions and terms. [134] Nevertheless, the exclusion of liability could be subject to an evaluation under the Unfair Contract Terms Act 1977 when the term is "unreasonable" and the Unfair Terms in Consumer Contracts Regulations 1999 when the term is "unfair".[135] The banks have the right to include their contracts with the customers term to exclude liability, but only if this term is deemed reasonable and fair.[136] Thus, it is time to give attention to this problem by

[133] Wang, *op.cit*., pp. 32-33.
[134] For example, see Lloyds TSB, Personal Banking terms and conditions 2012, section 8.4 http://www.lloydstsb.com/media/lloydstsb2004/pdfs/personal_banking_terms_and_conditions.pdf; HSBC, General Terms and Conditions, Current Account Terms and Conditions 2012, section 9 http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf; Barclays, Customer Agreement 2012, section 11http://www.barclays.co.uk/ImportantInformation/TermsandConditions/P1242575350746 13 February 2013.
[135] Unfair Terms in Consumer Contracts Regulations 1999 (SI 1999/2083).
[136] Unfair Contract Terms Act 1977, Schedule 2.

determining customers' and banks' liabilities for the authentication of unauthorized transactions and for both to agree with regard to their liabilities.

3.3.2.3 The legal validity and recognition of electronic signatures as a signature

The forms of security procedure are still not regulated by particular statutory instruments relating to EFTs. Such an absence is understandable given the rapid pace of technological change. From time to time new security procedures are created and so it is not easy to establish particular legal provisions to deal with particular items of security procedure. Nevertheless, this absence of statutory instruments leads to the problem of determining the legal validity of an encryption device. The use of a lawful security procedure is not sufficient grounds for considering the instruction to have been authorized.[137] Accordingly, a security procedure could be regarded as good evidence that the lawful customer authorized the transaction without such evidence affecting the parties' liability in the EFT transaction, which is the same as their liability when the payment instruction is in the form of a handwritten signature.

Under UK law there are two kinds of legislation governing the validity of security procedures: the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002.[138] Both laws regulate the legal validity of the security procedures,[139] irrespective of the kind of transaction the security

[137] PSR 2009, regulation 62(3).
[138] The Electronic Signatures Regulations 2002 (SI 2002/318) replaced the Electronic Signatures Directive 1999 (1999/93/EC)) OJ L13.
[139] Section 7(1) of the Electronic Communications Act 2000.

procedures are used for. Therefore, security procedures such as passwords, electronic signatures and TTP are legal and admissible in the context of EFT.

Indeed, section 7(1) of the Electronic Communications Act 2000 provides that an electronic signature, and the certification by a third party of such a signature, are each acceptable in evidence and also in proving the authenticity of the communication of data and the integrity of the communication of data. Nevertheless, the Electronic Communications Act 2000 comes without any indication to the legal effect of electronic signatures,[140] therefore, the courts will have the final decision and such decision will be in accordance with the particular circumstances, including such factors as evidential value, [141] for example, whether an electronic signature fulfils the legal requirements to qualify as a signature within specific regulatory contexts, and the relationship between the parties: the signatory, the certification service-providers and the relying party.[142] The Electronic Signatures Regulations 2002 establish liability of the certification service-providers for any damage or losses when the customer is proved to have taken all the reasonable steps and there is no negligence in his act.[143] The Regulations 2002, however, came without any indication as to the liability of TTPs who decided not to provide certificates; therefore, it is the

[140] Wang, *op.cit.,* p.38; Hogg, M., 'Secrecy and signatures-turning the legal spotlight on encryption and electronic signatures', (2000) *AHRC Research Centre for Studies in Intellectual Property and Technology Law* 1 at p. 5 http://www.era.lib.ed.ac.uk/bitstream/1842/2291/1/75_hoggsecrecyandsignatures00.pdf 19 February 2012.
[141] Robertson, et al., *op.cit.*, p. 340.
[142] Wang, *op.cit.,* p. 38.
[143] Electronic Signature Regulations 2002, regulation 4(1)(d).

courts' duty to determine the liability of such providers under common law rules.[144]

In the UK, there is no statutory definition for the signature which might assist in providing a decision as to whether or not electronic signatures and passwords are to be considered as signatures in the traditional sense.[145] Case law has drawn analogies between handwritten signatures and other types of authentication.[146] The "function approach" and the "form approach" are the two approaches adopted to determine the legitimacy and efficacy of a signature.[147] The "form approach" is used to define whether the signature is in the requested form, for instance, the initials of the person's name or his surname.[148] The "function approach", on the other hand, is used to define the function of a signature by examining its purpose and comparing it with other techniques which may be said it performs similar functions. According to the ""function approach" it may result that any type of signature or technique fulfilling the same function is considered to be a signature. Robertson et al have stated as follows:[149]

> "If a functional approach is taken to what constitutes a signature there are strong arguments for recognising electronic signatures as true equivalents for all legal purposes: an electronic signature created using the more sophisticated techniques discussed above [symmetrical key encryption

[144] Robertson, et al., *op.cit.*, p. 341.
[145] Reed, C., 'What is a signature?', (2000) 3 *Journal of Information, Law and Technology* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed 20 February 2012.
[146] *Goodman v J Eban Ltd* [1954] 1 Q.B. 550; *Firstpost Homes Ltd v Johnson* [1995] 1 W.L.R. 1567.
[147] Reed, *op.cit.*
[148] *Ibid.*
[149] Robertson, et al., *op.cit.*, p. 343.

> and public key encryption][150] is much more difficult to forge and, in that sense, more reliable a proof of identity than a handwritten signature."[151]

Thus, the e-signature is legal if it achieves the functions of a signature, regardless of the form it takes.[152] The English courts have adopted the "function approach",[153] and recognise e-signatures as the legal equivalent of manual signature.[154] Before 2006 the English courts identified the e-signature by drawing an analogy between it and the manual signature,[155] which held that the legal position of the e-signature was equivalent to the manual signature. But after 2006 such a view was challenged by two cases and the English's courts held that e-signatures are legal and equivalent to the manual signature. In *Pereira Fernandes SA v Mehta,*[156] the issue was, first, whether an email sent from the defendant's e-mail account, on his orders, constituted as equivalent to a note or memorandum of an alleged guarantee to meet section 4 of the Statute of Frauds 1677[157] and, secondly, whether the presence of the defendant's e-mail name find on the copy of the e-mail constituted an adequate signature for the purpose of section 4 of the Statute of Frauds 1677. The court held that a person could attach a signature sufficient to satisfy the requirements of the Statute of Frauds 1677 by any combination such as letters and numbers, providing always that whatever was used was inserted into the document in

[150] The words in square brackets added.
[151] Robertson, et al., *op.cit.*, p. 343.
[152] Reed, *op. cit.;* Angel, *op. cit*.
[153] *Goodman v J Eban Ltd* [1954] 1 Q.B. 550. The Court of Appeal, by a majority, recognised a signature produced by means of a rubber stamp as considering a sufficient. Per Lord Evershed M.R. at p. 557. See also *Good Challenger Navergante SA v Metalexportimport SA* [2004] 1 Lloyd's Rep. 67.
[154] *Derby & Co Ltd v Weldon (No. 9)* [1991] 1 W.L.R. 652; *IR Commrs v Conbeer & Anor* [1996] B.C.C. 189.
[155] Reed, *op.cit.*
[156] *Pereira Fernandes SA v Mehta* [2006] 1 W.L.R. 1543.
[157] Section 4 of the Statute of Frauds 1677 provides that contracts of guarantee (surety for another's debt) are unenforceable unless evidenced in writing.

order to give, and with the intention of giving, authenticity to it. Thus, regardless of the method and the form used, the most important factor was the intention.[158] On this ground, where the deliverer's name was only automatically attached to the delivered document by the e-mail system, the significant element of purpose, that of authenticating the content of the email, was absent, and therefore the requirements of the Statute of Frauds 1677 were not met. The second case was *Orton v Collins,*[159] which raised the following issue: whether writing the sender's name at the end of an e-mail was enough to meet the requirement of the Civil Procedure Rules 1998 (CPR)[160] in constituting a signature. It is logical for the email receiver to presume that the name written was added intentionally; provided that the e-mail has no programs which can automatically write the name at the end of the letter. It follows that the courts have a duty to investigate whether the email system was programmed to add the name automatically in order to decide which authorities apply to the case in question.

It has been proposed that the current difficulty in defining electronic negotiable instruments such as bills of exchange is the requirement for writing rather than the requirement for a signature.[161] Writing has been defined within Schedule 1 of the Interpretation Act 1978 as containing: "typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form". Bainbridge[162] argues that the detail saved in an electronic form is a document. Furthermore, an electronic record of computer data is unobservable

[158] *Ibid.*
[159] *Orton v Collins* [2007] 1 W.L.R. 2953.
[160] Civil Procedure Rules 1998 (1998/3132), Part 36 offers to settle.
[161] Bainbridge, D., *Introduction to Information Technology Law* (2008), p. 359.
[162] *Ibid.*

unless made so by a computer process upon it, such as print on paper.[163] Thereby applying the Interpretation Act 1978 definition to an electronic record requires the additional gloss of: capable of being made visible.[164] Riefa[165] agrees with O'Connor and Brownsdon[166] that digital signatures are now removed from the normal methods of signature, and examples range from writing a name to the more sophisticated biometric techniques such as fingerprint scanning.

Finally, given the situation described above, it seems that there is flexibility in the existing law: any security procedures used by the customer could be acceptable in evidence regarding the authenticity and integrity of the communication or data.[167] Therefore, there is no need for legislation to establish emails and internet website pages as writing as defined by English Law.[168] On this basis, the author's view is that the security procedures under English law are legal.[169] However, even with the legal validity of security procedures used to authenticate the payment instruction, the problem of identity authentication and its legal impacts on the customer's and the bank's liabilities for authenticated but unauthorized EFT instructions continue to leave room for debate and no final solution to the problem has been found.

---

[163] *Ibid.*
[164] *Ibid.*
[165] Riefa, C., and Hörnle, J., The Changing Face of Electronic Consumer Contracts in the Twenty-First Century: Fit for Purpose?, in Edwards, L., and Waelde, C., *Law and the Internet* (2009), pp. 98-99.
[166] O'Connor, M., and Brownsdon, E., 'Electronic signatures', (2002) 152 *New Law Journal* 348 at p. 384.
[167] The Electronic Communications Act 2000, Part 2, section 7(1)(a) and (b); and the PSR 2009, regulation 60; Hogg who argues that there is flexibility in the existing law thus; any new methods could be acceptable as signatures. Hogg, *op.cit*., p. 5.
[168] Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions*, December 2001, at pp. 8-12 www.lawcom.gov.uk 13 February 2013.
[169] Further, see Murray, J., 'Public key infrastructure digital signatures and systematic risk', (2003) 1 *Journal of Information, Law and Technology* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/murray/?textOnly=false 7 March 2012.

3.3.2.4 Liability of Certification Authorities and E-signatures

In practice, the lawful holder of the Certification Authority (CA) could be found in some cases to have used certification in an unauthorized way.[170] For example, where there is no suitable and adequate method of verifying the identity of the CA's holder[171] or where there is misappropriation of an e-signature and such an abuse is presented for transmission by a fraudster. The question arising is: who bears liability for such misappropriation or fraud? Reed has observed that "the obligations of CAs and the extent of their liability under existing law are difficult to determine".[172] He adds that within English law, the CAs can only be held liable according to contractual liability or tortious liability.[173] There is a contractual relationship between the CA and the user but there is no contract agreement between the CA and the relying party. Further question that needs to be asked, however, is whether a relying party who is not party to the contract and sustained losses as a result of a CA negligence has the right to sue the CA? Regulation 4 of the Electronic Signature Regulations 2002 has determined the liability of certification service-providers, and determines their duty of care to the relying party.[174] Such duty also covers the accuracy of the certification information. Conversely, if the issuer fails to protect the certificate by reason of negligence[175] or defaults to cancel the certification,[176] as in a case where there

[170] Hedley, S., *The Law of Electronic Commerce and the Internet in the UK and Ireland* (2006), p. 110.
[171] Schellekens, M., *Electronic Signatures Authentication Technology from a Legal Perspective* (2004), p. 102.
[172] Reed, C., *Internet Law* (2004), p. 161.
[173] *Ibid.;* Balboni, P., 'Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication', (2004) 13 *Information & Communications Technology Law* 211 at p. 212.
[174] Electronic Signatures Regulations 2002, regulation 4(1)(d).
[175] *Ibid.,* regulation 4(1)(d).

is suspicion regarding the security of the signature, that issuer will be liable to the rightful holder for any loss or damage. However, under Electronic Signature Regulations 2002 regulation 3, it is the customer who bears the burden of proof that the certifier is negligent, although the issuer bears no liability if it is established that he acted without any negligence.

An e-signature is not always supported by a CA, thus, in this regard the common law rules are still significantly involved:[177] firstly, the signer may be responsible for applying the rules of apparent authority or estoppel, when for example, there is a representation or holding out on the part of the signatory, rather than on the part of the fraudster.[178] Furthermore, it may be established that the signer is in breach of an obligation to exercise reasonable care and skill owed to the relying party if, for example, the signatory not only acted negligently in relation to the theft of the signature but also if there has been any representation made by the signatory to, or supposing the liability towards, the relying party.[179] Robertson et al clarifies that:

> "the party whose signature it is may be liable applying the principles of ostensible authority or, estoppel, or may be found to be in breach of a duty of care owed to the other party. The former will depend on there being a representation or holding out by the signatory, as opposed to by the fraudster. The latter will depend not only on whether the signatory was careless in relation to the theft of the signature but also on whether there has been any representation made by the signatory to, or assumption of responsibility towards, the relying party, which may well not be the case."[180]

---

[176] *Ibid.,* regulation 4(3)(c).
[177] Robertson, et al., *op.cit.*, p. 350
[178] *Ibid.*; Balboni, *op.cit*., at p. 217.
[179] *Ibid.*
[180] *Ibid.*

Nevertheless, within common law rules the party's e-signatory has no liability for any misuse or unauthorized use of the signature if the party's e-signatory has no duty to exercise reasonable care and skill.[181] In contrast, the party's e-signature liability may be included in the contracts' terms.[182] Secondly, the TTP who had certified the signature is subject to the rule in *Hedley Byrne and Co v Heller and Partners*.[183] In this case, the defendant bank (the representor) was aware that the negligent misstatement, about the financial stability of one of its customers, would be relied upon by the claimants (the relying party), who wanted to know it they could safely extend credit to the bank's customer in a substantial sum. In other words, the defendants had in mind reliance by the specific claimants, to whom the statement was made directly, for a particular transaction. According to *Hedley Byrne and Co v Heller and Partners*, a duty of care would be owed by the representor to the relying party if the representation was made intentionally to consider the representor liable to the relaying party. However, the representor who was negligent would be liable to the relying party for any monetary or personal damage caused to the relying party, but where the representor had expressly excluded liability for reliance on his statement no liability arose. Thus, the representation must have been made intentionally to consider the representor liable to the relaying party, even if he was negligent. [184] To consider a TTP who had certified a signature liable under *Hedley Byrne and Co v Heller and Partners,*[185] the relying party on the certificate can show both the existence of a duty of care and breach. This position will be applied if, for

[181] *Ibid.*
[182] Reed, *Internet Law, op.cit*., p. 161.
[183] *Hedley Byrne and Co v Heller and Partners* [1964] A.C. 465.
[184] *Ibid.*
[185] *Ibid.*

example, the TTP issued or verified the certificate, upon the demand of the relying party, after the TTP had been given notification of cancellation, since there will then have been a negligent misrepresentation made straight to the relying party in circumstances where the relying party was intended to place reliance on the certificate.[186] Therefore, there is no liability of the certifier who has not assumed any obligation towards the relying party, even if the certifier acted in a negligent way: for example, the relying party relies on a certificate for a purpose outside its stated terms, or the relying party fails to verify a certificate which invites him to do so and this would have disclosed that it was no longer valid, or the fraud was undetectable by the certifier exercising reasonable care, who therefore did not breach any duty by certifying the impostor's signature.[187]

It is submitted that there is apparent authority where, for instance, an employee may have the right to access and use the employer's e-signature for a legal transaction, thereby using an e-signature without the customer's authority, giving rise to the employer's e-signatory liability.[188] EFT transactions have not been executed, or executed in the wrong way, due to the act or failure of the bank or of the banks' employees. The bank is only liable when losses or risk result from its employee's fraudulent or negligent execution during the course of their employment.[189]

It is indisputable that an e-signature can function as a representation in legal situations; the signer of a document has no right to deny its liability. Moreover,

[186] Robertson, et al., *op.cit.*, p. 350.
[187] *Ibid*.
[188] *Ibid.*, at p. 351.
[189] See section 3.4.2.3 below.

common law rules[190] emphasise that a party who has contributed to an unauthorized use of an e-signature has no right to reject its liability for damages under tortious liability. There is a duty of care from the CA to the relying party to make certain the accuracy of the details in the certificate. If in default, the CA is to exercise a duty of care arising from liability for any losses that occur to the relying party. Therefore, under tortious liability any losses issuing from unauthorized encryption used between the transactions of the parties give rise to the liability of the negligent party. Robertson et al[191] have argued such a point:

> "In the absence of contractual terms to the contrary, it would seem probable that the negligent party (or the party whose agent the TTP was) would be liable to the other party in tort for reasonably foreseeable losses, on the basis of breach of a duty of care (or vicarious liability for the TTP's breach of such a duty)"

Given the above position, it seems that there are no particular statutory provisions determining liability for a CA. However, a relying party has two possibilities of an action against a CA. First, based on the contractual relationship between the certificate authority and the relying party, a relying party has a cause of action resulting from any breach of the contract terms and conditions. Secondly, there is an action in tort on the basis that the certificate authorities or relying party acted in a negligent way in ascertaining the accuracy of the details in the certificate. Where an e-signature or encryption has been compromised, the consequence of such a compromise will be that a consumer's payment instrument is used without authorization by a third party. In

[190] *Lloyd v Grace, Smith &Co* [1912] A.C. 716; *Armagas Ltd v Mundogas SA (The Ocean Frost)* [1986] A.C. 717: *First Sport Ltd v Barclays Bank Plc* [1993] 1 WLR 1229; *Greenwood v Martins Bank Ltd* [1933] A.C. 51; *Standard Bank London Ltd v Bank of Tokyo Ltd* [1995] C.L.C. 496.
[191] Robertson, et al., *op.cit.*, p.352.

such a case, unless the third party acted with the customer's authority the customer will be liable to the issuer for any unauthorized transactions under the CCA 1974 [192] or the Consumer Protection (Distance Selling) Regulations 2000.[193] In addition, under the PSR 2009 one of the bank's duties, imposed by the Regulations 2009, is to protect the customer security procedures for a payment device. It also sets narrow rules on the customer's liability for misuse.[194]

3.4 EFT parties' liability for unauthorized transactions

Fraudulent, stolen cards and PINs and misuse of cards lead to unauthorized EFT instructions. In fraudulent payment instructions which are unauthorized EFT, the person who initiates the instruction is either the person who is authorized to initiate such an instruction or a person who is not authorized to do so. This person could be the customer's employee, the bank's employee or a third party.[195] Nevertheless, this person could be the customer himself if he acted fraudulently or with fraudulent intent or with gross negligence.[196]

The basis of the customer's action against his bank for an unauthorized payment transaction is "founded on simple contract",[197] given that the customer-bank relationship is a contractual relationship. Thus, if the paying bank debits its

[192] CCA 1974, section 83(1).
[193] The Consumer Protection (Distance Selling) Regulations 2000 (SI 2000/2334) amended by The Consumer Protection (Distance Selling) (Amendment) Regulations 2005 (SI 2005/689).
[194] PSR 2009, regulation 58(1); Further, see 4.4.2.4 section below.
[195] Lass, J. D., 'R., 'Fraud, Error and System Malfunction' in Goode, R., *Electronic Banking: The Legal Implications* (1985), pp. 59-60.
[196] PSR 2009, regulation 62(2).
[197] *National Bank of Commerce v National Westminster Bank Plc* [1990] 2 Lloyd's Rep. 514 at p. 516

customer's account without the customer's mandate (unauthorized payment order), the paying bank breaches its duty under the contract by making payment outside the customer's mandate. Such a point is demonstrated in *National Bank of Commerce v National Westminster Bank Plc,*[198] where the defendant debited the claimant's account with £268,227.08 in respect of eight mail transfer orders, (MTOs), purporting to have been signed by two authorized officers of the claimant. The claimant alleged, but the defendant denied, that none of the MTOs was in fact signed by two authorized officers and that the debits were therefore erroneous. In determining whether the customer's right against his bank depended on contract or tort, the court held that the claim for the principal funds is not based on an action in tort: it exists only in the agreement between the parties. It is, therefore, an action founded on simple contract.[199] Thus, the customer has two claims against the bank according to this "simple contract". Webster J. held:

> "The points of claim, on their face, contain, apart from the declarations, two sets of claims founded on contract: first, a claim to be repaid the principal sum in respect of which the defendant is alleged to be indebted to the plaintiff following a demand to repay that sum, and a similar claim in respect of interest on that sum; and secondly, a claim for damages for breach of the obligation, under the "agreement governing the account", to repay each of those two sums." [200]

By analogy, if the paying bank debited the payer's account according to the unauthorized EFT the payer has the right to make a claim on the bank for a breach of the bank's duty under either the creditor-debtor relationship or the agent-principal relationship, as explained in chapter two, and consequently the payer has the right to charge the paying bank for the original funds which have

[198] *National Bank of Commerce v National Westminster Bank Plc* [1990] 2 Lloyd's Rep. 514.
[199] *Ibid.,* at p. 516.
[200] *Ibid.*

been paid and the interest. Furthermore, the payer may be authorized to claim for damages, but only if that is in accordance with the account agreement.[201]

Currently, with the implementation the PSR 2009, reciprocal obligations and liabilities for both the bank and customer in relation to unauthorized transactions are covered.[202] Regulations 57-58 present reciprocal obligations for both the bank and customer in relation to payment instruments. The customer is required to use the payment device in accordance with the specific terms and conditions of the contract and to take all skill and care to protect the security payment device.[203] Furthermore, the customer is required to inform his bank instantly on becoming aware of the loss, theft, misappropriation or any unauthorized use of the payment instrument. In turn, the bank issuing a payment instrument is under the following obligations:[204] firstly, to protect and prevent any access to the security procedures of the cards, other than the customer to whom the card has been issued;[205] secondly, to abstain from sending an unwanted payment instrument other than as a replacement to a current one;[206] thirdly, to guarantee that a suitable means is always available to enable the customer to make required notifications in case of loss, theft, or misappropriation of the payment instrument; [207] fourthly, to cancel the payment device directly after the notification.[208] Part 6 of the PSR 2009 applies to the authorization of a payment instruction and establishes legal norms applying to the EFT parties' obligations and liabilities. Nevertheless, the PSR 2009 provides no solution to a number of

[201] *Ibid.*
[202] PSR 2009, Part 6.
[203] *Ibid.*, regulation 57.
[204] *Ibid.*, regulation 58.
[205] *Ibid.*, regulation 58(1)(a).
[206] *Ibid.*, regulation 58(1)(b).
[207] *Ibid.*, regulation 58(1)(c).
[208] *Ibid.*, regulation 58(1)(e).

problems stemming from unauthorized EFT instructions, for example, those relating to the duty to exercise care and skill, ambiguous EFT instructions and the duty to take reasonable care to prevent opportunities for fraud. Finding solutions to these problems is important: (1) in determining what obligations the customer has towards the bank and what obligations the bank has towards the customer; (2) in deciding whether it was the bank or the customer who defaulted in the performance of their duty to exercise reasonable care and skill.[209] The answer to these problems can be found in the principles of common law, namely, contract law and agency law.[210] Thus, the common law principles will be examined. Accordingly, the following pages will examine the customer's liability for unauthorized EFT transactions and the ambit of the bank's liability for unauthorized EFT transactions under the existing law.

3.4.1 Customer's liability for unauthorized EFT transactions

The customer's liability for unauthorized payment transactions, lost or stolen cards, or default in protecting personalized security features of cards is enshrined in regulation 62 of the PSR 2009 in cases where EFT transactions fall within its scope. Regulation 57 enshrines the customer's obligations in relation to payment transactions, to abide him by the terms and conditions regarding the use of the relevant payment instrument. Although, regulation 51(3)(a) establishes that where the customer is not a consumer, a micro-

[209] Mason, S., *Electronic Banking: Protecting Your Rights* (2012), p. 37.
[210] Ellinger, E., et al., *Modern Banking Law* (2011), p. 668; Geva, B., *Legal Aspects Relating to Payment by E-Money: Review of Retail Payment System* (2001), p. 25; Wadsly, J., and Penn, A. G., *The Law Relating to Domestic Banking* (2000), p. 103.

enterprise or a charity, the parties have the right to agree not to apply regulation 62.

CCA 1974, sections 84 and 66 apply on cards subject to the Act 1974, for example, credit cards' and charge cards' loses. The difference between the CCA 1974 and the PSR 2009 is with the applications. To prevent the re-application repetition, payment transactions covered by the CCA 1974 do not apply the PSR 2009, for example, card issued under credit token agreement applies CCA 1974. There are salient differences in the liability of cards misuse, as will explain. Under the PSR 2009 the customer's liability for unauthorized EFT transactions addresses as follows:

(1) The customer is liable for loss due to unauthorized transactions up to £50 and the card issuer bears any losses that exceed £50. It is worth mentioning that this narrow liability runs regardless of the customer's mistakes and regardless of the customer's lack of knowledge of the unauthorized transactions.[211]

(2) It is the customer's duty to inform his bank 'without undue delay' upon becoming aware of the unauthorized nature of the transaction, and the delay can never exceed 13 months from the date debited the customer's account.[212] Where a customer is a business, the parties (bank-customer) may agree that a different time period applies.[213] There is no liability of the customer if the losses incurred due to an unauthorized payment occur after the customer informs the bank, provided that not more than 13 months have elapsed since

[211] PSR 2009, regulation 62(2)(B), and CCA 1974, sections 83(1) and 84(1), (2) and (3).
[212] *Ibid.,* regulation 59(1).
[213] *Ibid.,* regulation 51(3)(b).

the charge date.[214] While under the CCA 1974, the card holder can make a claim of unauthorized payment at any proceeding brought within the limitation period, although delay in raising a challenge will undermine credibility.[215]

(3) There is no liability of the customer if the losses incurred due to an unauthorized payment occur as a result of the bank failing to provide the customer with the appropriate means of notification.[216]

(4) The customer is completely liable for all losses if he acted fraudulently or with "gross negligence" and the paying bank can prove that such was the case,[217] and this is so even if the CCA 1974 otherwise applies.[218]

Given the above position, it appears that the best interpretation of a customer's liability up to £50 and his liability for unlimited losses is that the customer bears losses for unauthorized transactions after notification only on condition that he has acted in a fraudulent or grossly negligent way. The customer must inform his bank 'without undue delay' upon becoming aware of the unauthorized payment and this delay can never exceed 13 months from the date when the payer's account was debited with the payment.[219] Thus, it is debatable whether the customer may be considered grossly negligent when there is delay in informing the bank about the unauthorized transaction,[220] but such a view is justified when the customer bears all losses previous to the notification.[221] However, the reason behind emphasis the PSR 2009 on "gross negligence" is

[214] PSR 2009, regulations 59(1) and 51(3)(b).
[215] Smith, M., and Robertson, P., 'Plastic Money' in Brindle, M. and Cox, R., (eds), *Law of Bank Payments* (2010), p. 238.
[216] PSR 2009, regulation 62(3)(b).
[217] *Ibid.*, regulation 62(2).
[218] CCA 1974, section 84(3A), (3B) and (3C).
[219] *Ibid.,* regulation 59(1) and 51(3)(a).
[220] *Ibid.*, regulation 57(1)(b).
[221] *Ibid.*, regulation 62(2)(b); Geva, payment transactions under the EU Payment Services Directive: a U.S. comparative perspective, *op.cit.,* p.729.

to make the customer's obligation noticeably lighter.[222] Furthermore, regulation 60[223] places the burden of proof directly onto the bank to show that the unauthorized transaction was authenticated, exactly recorded and there was no technical breakdown. Even if the bank does this, the PSR 2009 go on to say that this is insufficient to proof that the payment was authorized or the customer was fraudulent or grossly negligent. [224]

The customer's liability for an unauthorized payment is determined by the conditions and terms of the agreement with the bank, and certainly by the general principles of the common law when the unauthorized payment falls outside the ambit of the PSR 2009. There are nevertheless a number of issues which need to be addressed in order to determine the customer's liability for unauthorized EFT instructions.

[222] Davies, *op. cit.,* p. 241.
[223] PSR 2009, regulation 60 and regulation 51(3)(a).
[224] Davies, *op. cit.,* pp. 241-242.

Table 2: Customer's liability for unauthorized use of payment instrument under PSR 2009.

Unauthorized use	Liability
Lost or stolen payment card, or card misused without permission, before card issuer has been informed	Up to £50
Lost or stolen payment card, or card misused without permission, once card issuer has been informed	No liability
payment card misused with permission (broadly equivalent to fraud or failure with intent)	Unlimited
Payment card lost, stolen or misused because of holder's gross negligence	Broadly equivalent to "without reasonable care" – unlimited, unless the card was used as a credit token, for example, credit card, in which case £50 limits applies

3.4.1.1 The duty of exercising care and skill not to facilitate fraud

To determine the customer's liability for unauthorized EFT instructions it must be considered whether the customer is under a duty to take all reasonable care and skill towards his bank. In drawing the cheque the customer is obliged to execute reasonable care and skill to not to facilitate of forgery.[225] For instance, in *Young v Grote*[226] the court held that the customer should bear the losses of the cheque forged by one of his employees, since the customer took no reasonable care and skill in signing a blank cheque and this negligence gave a clerk the opportunity to fraudulently enter a sum in an empty space left on the cheque. Thus, in drawing the cheque the customer is obliged to execute reasonable care and skill, not allowing for any facilitation of forgery. [227] Regarding the duty of care and skill, the customer has to take usual and reasonable care to prevent cheque forgery.[228] But within EFT transactions, the picture is different; the payment instruction is issued and "signed" electronically. Accordingly, the customer's duty to exercise reasonable care and skill in issuing and signing the payment instruction takes a different for from drawing a blank cheque or leaving a space for words or numbers to be added so as to alter the cheque amount.

As a matter of fact, in the context of EFT, the customer's default or negligence could be participatory in the issue of payment instruction, for example by keeping the PIN and the card in the same place, fails to inform the bank

[225] Wadsley, J. and Penn, G., *The Law Relating to Domestic Banking* (2000), p. 241
[226] *Young v Grote* (1827) 130 E.R. 764: *London Joint Stock Bank Ltd v Macmillan* [1918] A.C. 777.
[227] Wadsley and Graham, *op.cit*., p. 241.
[228] *London Joint Stock Bank Ltd v Macmillan* [1918] A.C. 777 at pp. 789-790.

instantly of unauthorized payment after receiving notification of fund transfer from the bank.[229] However, the authorization of payment by cheque, which is normally done through a manual signature, is not the same as the method of authorizing an EFT and therefore the rules for the customer's liability for a forged cheque cannot apply to the customer's liability for EFT fraud. Also, the clear nature of electronic authentication is different from a manual signature.[230] Consequently, covering the rules of forged cheques to the payer and payer's bank's liability for fraudulent EFT drives to unpredictability and uncertainty in their liability. Geva has provided a convincing argument on this point.[231] He confirms that apply the rules of handwritten signatures to an electronic authentication are fundamentally useless because the nature of electronic authentication is different from that of a manual signature.[232]

The next issue involving the customer's duty to exercise reasonable care and skill is whether the customer is liable for his employees, including the exercise of care in the employment of personnel. According to the English cases, the customer's duty to exercise care and skill towards his bank is very narrow. [233] In *Kepitigalla Rubber Estates v National Bank of India*,[234] the court emphasized the narrow duty owed by the customer to the bank to exercise care and skill in the general conduct of business and in the examination and checking of pass-books, the court held that "there is a duty to use reasonable care in issuing the

[229] Geva, B., 'Consumer liability in unauthorized Electronic Funds Transfers, *op. cit*., pp. 228-231.
[230] *Ibid.*
[231] *Ibid.*
[232] *Ibid.*
[233] *Young v Grote* (1827) 130 E.R. 764; *London Joint Stock Bank Ltd v Macmillan* [1918] A.C. 777; *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] A.C. 80; *Financial Institutions Services Ltd v Negril Negril Holdings Ltd* [2004] UKPC 40.
[234] *Kepitigalla Rubber Estates v National Bank of India* [1909] 2 K.B. 1010 at p. 1029, presented by *Brewer v. Westminster Bank Ltd* [1952] 2 All E.R. 650.

mandate, but no further." [235] Furthermore the court held that 'to afford a defence to the banker the breach of duty must be, as in *Young v. Grote*, in connection with the drawing of the order or cheque, and that there is no obligation between customer and banker that customer should take precautions in the general carrying on of his business or in examining and checking the pass-book.'[236]

Regarding the 'narrow duty', the customer owed no duty to exercise care and skill towards his bank in the execution of business, including choice of employees, in order to discover or prevent forgeries. The customer's duty of care and skill towards the bank exists only if there is a term in the contract which expressly states such a duty;[237] otherwise the bank has no right to debit the customer's account and it will bear any losses resulting from cheque forgery. [238] In *London Joint Stock Bank Ltd v Macmillan* [239] Lord Finlay emphasized that the customer is under no duty to exercise reasonable care and skill in choosing his employees:

> "Of course the negligence must be in the transaction itself, that is, in the manner in which the cheque is drawn. It would be no defence to the banker, if the forgery had been that of a clerk of a customer, that the latter had taken the clerk into his service without sufficient inquiry as to his character. Attempts have often been made to extend the principle of *Young v Grote* beyond the case of negligence in the immediate transaction, but they have always failed."[240]

It seems that according to the common law, such as *Young v. Grote* and *London Joint Stock Bank Ltd v Macmillan* imposes, the customer's duty to toward his bank to exercise reasonable care and skill is a narrow duty confined

[235] *Kepitigalla Rubber Estates v National Bank of India* [1909] 2 K.B. 1010 at p.1022
[236] *Ibid*., at pp. 1022-1024.
[237] *Ibid.* p. 1025.
[238] *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] A.C. 80 at p. 110.
[239] *London Joint Stock Bank Ltd v Macmillan* [1918] A.C. 777 at p. 795.
[240] *Ibid.,* at p. 795.

to the conduct of banking transactions. As a result of such narrow duty, the customer is under no duty to exercise reasonable care and skill in carrying on business, including selecting employees, so as to detect or prevent forgeries;[241] secondly, the customer is under a duty to exercise reasonable care and skill in drawing the cheque in respect of writing and signing the cheque in order to prevent fraud.[242]

By analogy, in the EFT context, regulation 62(3) of the PSR 2009, when it is applicable as explained above, establishes the customer's liability for unauthorized payment transactions. Although, when the EFT transaction falls outside the ambit of the PSR 2009, there is no particular legislation governs the customer's liability for EFT fraud. Therefore, the author's view is that in the EFT context, the customer's duty to exercise reasonable care and skill to prevent fraud is a very narrow one. However, a customer is under a duty to inform his bank immediately once he becomes aware of the fraud.[243] Otherwise he may be found liable for facilitating a forgery if a customer fails or delays to notify the bank about the fraud. A bank may plead that its customer is personally estopped from asserting that the bank is not entitled to debit his account.[244] Regarding to the PSR 2009 the customer is under an obligation to inform his bank 'without undue delay' upon becoming aware of the unauthorized nature of the transaction, and the delay can never exceed 13 months from the date when

[241] *Ibid.,* at p. 795.
[242] *London Joint Stock Bank Ltd v Macmillan* [1918] A.C. 777; Geva, *Bank Collections and Payment Transactions, op.cit.,* p. 399; Ali Khan, L., 'A theoretical analysis of payment systems' (2008) 60 *South Carolina Law Review* 425 at p. 486.
[243] The degree of knowledge was considered by Arden J. in *Price Meats Ltd v Barclays Bank Plc* [2000] 2 All E.R. (Comm) 346. Further, see section 3.4.1.2 below.
[244] *Greenwood v Martins Bank Ltd* [1933] A.C. 51.

the payer was debited with the payment.[245] Furthermore, the customer is under a duty in protecting payment instruments and security procedures. Regulation 60 of the PSR 2009 establishes that use of the agreed security procedure is not necessarily a sufficient ground for considering that the payment is authorized and that the bank has exercised its duty of care and skill to execute the payment instruction.[246] When a customer claims not to have authorized an executed payment instruction it is the bank's duty to prove that the payment instruction was authenticated, accurately recorded and not affected by a software program breakdown or some other form of inadequate security. Thus, PSR 2009 exist a very narrow duty of customer to exercise reasonable care and skill to prevent fraud. In this regard, if the instruction is amended by one of the customer's employees after the rightful person has initiated the payment instruction it is uncertain whether the bank is authorized to debit the customer's account. The author's view is that the bank should accept the instruction and debit the customer's account as long as the payment instruction is authenticated, irrespective of whether it is an authorized payment instruction or not. Moreover, the author agrees that in EFT systems it is unacceptable to discharge the customer from the responsibility of taking all reasonable steps of care in the implementation of its business of preventing the computer terminal and PIN from being accessed by an unauthorized person. This view could be justified as follows: in EFT systems, an alteration to the payment instruction could happen for different reasons, such as a fraudster obtaining access to the computer terminal as a consequence of the customer's negligence. An EFT instruction could also be modified by the fraudster as a consequence of the

[245] PSR 2009, regulation 59(1) and regulation 51(3)(b).
[246] Further, see Mason, *op.cit*., p.39.

customer's negligence in keeping a card and its PIN or password in the same place. In an EFT transaction, the customer transfers an electronic instruction to the bank and the instruction appears on a computer screen. The bank will examine the instruction by comparing it with the security data it already has. The bank thereby passes the funds from the customer's account to the payee's account as an authorized instruction as soon as the payment instruction has been authenticated. Geva[247] argues that it is nonetheless difficult for the bank to determine the identity of the person who passed the instruction. Thus, if the payment instruction has not been transacted by the rightful person because the rightful person did not take all reasonable steps to protect his passwords or PIN, the customer would be responsible for the fraudulent EFT instruction and the bank would be authorized to debit the account.[248]

The customer's bank cannot debit the payer's account on a forged mandate, particular if there is no breaching of the customer's duty to the bank. If a bank debited its customer's account depending on forged EFT instruction, the payer will be entitled to request a recredit of the account.[249] In such case the payment is treated as made without authority. Given the above situation, it seems that there are insufficient norms applying specifically to EFT transactions. Ahmad argues this point:[250]

> "In the 21st century,...fraud is a major and global problem. By nature of its being global, its adverse effects are being experienced by all jurisdictions; however, it also impacts locally at a national level, for which we require legislation that tailors the remedy to the local needs."[251]

[247] Geva, Consumer liability in unauthorized Electronic Funds Transfers, *op.cit.,* pp. 232-233.
[248] *Ibid.*
[249] *Agip (Africa) Ltd v Jackson* [1991] Ch. 547; See chapter six, section 6.2.
[250] Ahmad, *op. cit*., p.114.
[251] *Ibid.*

The general principles of law applied to determining the parties' liability for unauthorized EFT instructions are for the most part formulated by analogy with the norms governing loss allocation in cases of forged cheques.[252] However, applying the norms of loss allocation in the case of forged cheques to the customer's and the bank's liability for unauthorized EFT transactions fails to provide predictability and certainty with regard to that liability.

3.4.1.2. Checking bank statements

The next issue relating to the customer's duty to exercise reasonable care and skill is whether the customer is liable for checking the bank statement. There is nothing under the PSR 2009, where it is applicable, referring to the obligation of the customer to check periodic bank statements. However, a customer seeking redness for an unauthorized or incorrectly executed payment transaction must inform his bank 'without undue delay' upon becoming aware of the unauthorized nature of the transaction, and this can never exceed 13 months from the date when the payer was debited with the payment, unless a different this period has been agreed. [253]

A bank customer does not have a general duty to check his or her bank statements, unless there is an express term in the banker-customer contract imposing such a duty on the customer.[254] In *Tai Hing Cotton Mill Ltd v Liu*

[252] Geva, *Bank Collections and Payment Transactions, op.cit.,* p. 393; Pennington, *op.cit*., p.67.
[253] PSR 2009, regulation 59(1) and regulation 51(3)(b).
[254] *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] A.C. 80; *Financial Institutions Services Ltd v Negril Negril Holdings Ltd* [2004] UKPC 40.

Chong Hing Bank Ltd,[255] Lord Scarman held that if banks wanted to include in their contracts with customers an express term imposing a duty to check periodic statements, such a term should specify in clear language that the customer must check the bank statement and inform the bank of forged cheques. Indeed, the bank is not authorized to debit the customer's account on the basis of the forged cheques.[256] His Lordship held:

> "If banks wish to impose upon their customers an express obligation to examine their monthly statements and to make those statements, in the absence of query, unchallengeable by the customer after expiry of a time limit, the burden of the objection and of the sanction imposed must be brought home to the customer."[257]

Although, it may be argued that the customer is generally in a much better position than the bank to check his or her bank statements and verify their accuracy. Therefore, it is argued that, as a matter of policy, the risk should fall on the customer.[258] Such view could be justified as follows: if a customer is under no duty to examine bank statements, then what is the purpose of sending a statement including detailed entries? If the aim is only to notify the customer of the funds standing to credit of his account, it would be adequate to send him periodically a statement of his balance without any detailed entries.[259] Here a statement without any detailed entries would be meaningless, because such statement gives the customer no information or details about his account. It gives the balance. But if the customer wants a statement including detailed entries, then certainly the customer can be expected to examine the statement

[255] *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] A.C. 80.
[256] *Ibid.,* at p. 110.
[257] *Ibid.*
[258] *Arrow Transfer Co Ltd v Royal Bank of Canada* [1972] R.C.S. 845, per Laskin J.
[259] Ellinger, et al., *op.cit.,* p. 239.

with a view to discovering errors or shortfalls.[260] This point is well demonstrated in the Supreme Court of Canada case of, *Arrow Transfer Co Ltd v Royal Bank of Canada.*[261] In this case, Laskin J. is a disunity opinion, held that the customer is under a duty to examine bank statements and to report any discrepancies within a reasonable period.[262] Indeed, in the United States of America, the Uniform Commercial Code, in section 4-406 imposes on the customer a duty to 'exercise reasonable cares in examining the statement or the items to detect whether any payment was not authorized and the customer must immediately inform the bank of the relevant facts.' Accordingly, if the customer fails to examine his bank statement and the he sustains loss as a result; the customer has no right to recover the loss attitudes to the unauthorized. Nevertheless, this estoppel does not apply, if the customer proves that the bank was negligent and in all case this can never exceed one year from the date when the customer received his statement.[263]

The position in English law stands in strong contrast to the position in the United States. In the UK, the common law submits that the customer is under no duty to check a bank statement unless there is a "verification clause" included in clear and unambiguous terms in the contract.[264] Although, if a bank customer becomes aware that an entry made in his or her bank statement is wrong, but remains silent, then he or she will be estopped from asserting the error once the bank has changed its position. In other words, by analogy with the rules applying to forged cheques, if a customer fails to notify, or delay notifying, the

[260] *Ibid.*
[261] *Arrow Transfer Co Ltd v Royal Bank of Canada* [1972] R.C.S. 845, per Laskin J.
[262] *Ibid.,* at pp. 870-871, per Laskin J.
[263] The Uniform Commercial Code, section 4-406(f).
[264] *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] A.C. 80.

bank about a fraud, the bank can use the defence of estoppel if the customer then sues the bank seeking the return of the funds. This point is well illustrated in *Greenwood v Martins Bank Ltd*;[265] in this case a customer discovered that his wife had been forging his signature on cheques drawn on his account. The customer was persuaded by his wife not to inform the bank about the forgeries. Several months later, his wife revealed that she had lied to him about the actual reason that she had forged his signature. Therefore, he changed his mind and decided to tell the bank about the forgeries. The wife then committed suicide and after her death he sued the bank for paying the cheques in breach of mandate. The bank used the defence of estoppel against the customer on the ground that the customer had breached his duty to notify the bank of the forgeries as soon as he became aware of them. The Hose of Lords held in favour of the bank.[266]

But, the difficult issue is whether estoppel should also apply in a case where the customer did not have actual knowledge of the wrongful entry, but on the ground of any reasonable practice or common sense ought to have identified or suspected it. This point is well illustrated in *Price Meats Ltd v Barclays Bank Plc* by Arden J.[267] In this case the plaintiff company brought legal action against the defendant bank in respect of cheques drawn on the plaintiff's account, the signatures on which were apparently forged. The bank's defence was that the customer had failed to exercise its duty to notify the bank of forgeries of which it had constructive knowledge. In this case Arden J. considered the degree of knowledge and held that constructive knowledge in the sense that the customer

[265] *Greenwood v Martins Bank Ltd* [1933] A.C. 51, at p. 57.
[266] *Ibid.,* per Lord Tomlin.
[267] *Price Meats Ltd v Barclays Bank Plc* [2000] 2 All E.R. (Comm) 346.

had the means of knowing of the forgery was not adequate. What is indeed is actual knowledge or shutting one's eyes to an obvious means of knowledge.[268] Furthermore, in *Patel v Standard Chartered Bank*,[269] the court held that 'although a customer was under a duty to inform his bank of any fraud or forgery as soon as he became aware of it, which included wilful blindness, that duty did not include reporting fraud about which the customer as a reasonable person ought to have been put on inquiry. To impose a duty to inquire and report based on knowledge of circumstances which would cause a hypothetical reasonable customer to discover the existence of fraud was unsound in principle and inconstent with authority'.[270] Although, the borderline between constructive knowledge and actual knowledge, much depends on the circumstances of each case and it remains unclear. For example, in *Morison v London County and Westminster Bank Ltd,*[271] the court supporting the proposition that constructive knowledge may be sufficient to raise an estoppel. A further example is *Brown v Westminster Bank Ltd,*[272] in such case the customer was an old woman who could not take care of her own business. Her servant forged her signature on cheques drawn on her account. The bank called the woman several times to ask verification the cheques. Nevertheless the woman did not expressly examine the signature on the cheques also she refrained from questioning their payment. Therefore, she held to be estopped from denying the bank's right to debit her account. However, Ellinger agrees that 'it is to be doubted whether conduct falling short of that in *Brown*, which

[268] *Ibid.*, at pp. 348-350.
[269] *Patel v Standard Chartered Bank* [2001] Lloyd's Rep. Bank. 229.
[270] *Ibid.; Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] A.C. 80; *Price Meats Ltd v Barclays Bank Plc* [2000] 2 All E.R. (Comm) 346.
[271] *Morison v London County and Westminster Bank Ltd* [1914] 3 KB 356, per Phillimore L.J.
[272] *Brown v Westminster Bank Ltd* [1964] 2 Lloyds Report 187.

acted to lull the bank into a false sense of security about the cheque, will be sufficient to found an estoppel'.[273]

In the final analysis, to make the customer liable, the bank must prove that the customer has actual knowledge of unauthorized transactions, but initially did nothing to inform the bank of the forgery.[274] In practice, banks commonly write into their contracts with customers a clause specifying the customer's duty to examine monthly bank statements for unauthorized transactions.[275] According to this clause, the customer is liable for unauthorized payment transactions taking place after the receipt of the bank statement, only if such an unauthorized payment could have been avoided by informing the bank.[276] However, if such a verification clause is included in a standard for banking contract, it could still be open to challenge on the ground that it is "unreasonable" under the Unfair Contract Terms Act 1977 or "unfair" under the Unfair Terms in Consumer Contract Regulations 1999.

When the customer's liability to check bank statements exists, the bank is under an obligation to dispatch bank statements to the customer, although the frequency of the statements depends on the agreement made between the two parties concerned. In recent times various options have been established for obtaining bank statements. This can now be done by telephone or via the internet if the customer has an online account. An online statement is free but

[273] Ellinger, et al., *op.cit.,* pp. 247-248.
[274] *Genki Investments International Ltd v Ellis Stockbrokers Ltd* [2008] 1 B.C.L.C. 662, paras, 44-46.
[275] Lloyds TSB Bank Personal Banking Terms and conditions [5.5] http://www.lloyds.com/Common/Help/Terms-and-conditions 20 July 2012; HSBC Bank General Terms and Conditions [26.4] http://www.businessgrant.hsbc.co.uk/terms 20 July 2012.
[276] John F. Dolan, 'Impersonating the drawer: a comment on professor Geva's consumer liability in unauthorized Electronic Funds Transfers', (2003) 38 *Canadian Business Law Journal* 282 at p. 290.

some banks may charge for presenting a telephone statement on a weekly or monthly basis. In these cases the courts will consider that the customer is not negligent if he exercises ordinary care and skill to prevent fraud by checking the bank statements. The final question involving a bank statement is whether a bank statement should be treated as an "account stated" for the purpose of legal proceedings. Normally the argument of considered a bank statement as an account stated creates by the party that willing to be free from liability against the other. In the strict sense of the term, an account stated clarifies the position where an account contains items both credit and debit, and the data are adjusted between the parties and a balance struck.[277] English courts have held that bank statements do not qualify as an "account stated".[278]

In conclusion, unless the contract between the customer and the bank establishes the customer's duty of care, the customer owes the bank only a narrow duty to exercise care and skill[279] not to facilitate fraud,[280] protecting his payment instrument and security procedure, and informing his bank immediately once he becomes aware of the fraud. When the customer's liability to check bank statements exists he is under a duty to check the bank statements otherwise if such duty not exist he is not. Indeed the customer is under no duty to his bank in the choosing and selecting of his employees. Finally, it is the bank's duty to prove that the customer acted negligently of fraudulently when initiating the payment instruction to make a customer liable.

[277] *Siqueira v Noronba* [1934] A.C. 332, per Lord Atkin at p. 337.
[278] *Bank of England V Vagliano Bros.* (1891) AC 107, at pp.115-116; *Chatterton v London and Country Bank, The Times,* 21 January 1891.
[279] Marten, R., 'The customer's duty to take care in the exercise of an account: a criticism of Tai Hing Cotton Mills v. Liu Chong Hing Bank Ltd', (1986) 2 *Professional negligence* 17 at p. 19; Davies, *op.cit.,* p. 242.
[280] Davies, *op.cit.,* p. 242.

3.4.2 The bank's liability for unauthorized EFT Transactions

The payer's bank[281] is obliged to execute the payer's EFT instruction only with the customer's consent.[282] Within Part 6 of the PSR 2009[283] the payer's bank is liable to the payer for redress only when the customer informs the bank immediately on becoming aware of an unauthorized or wrongly executed EFT instruction. [284] Such notification must be no later than 13 months after the charge date. [285] The payer's bank is also liable to the payer when it has executed a payment transaction without the payer's authorization[286] or when the customer has cancelled the payment instruction before it is completed.[287] In these circumstances the bank will be liable for refunding the amount of the transaction. Nevertheless, the bank is under no duty to execute its customer's instruction if the payment instruction was issued with an incorrect 'unique identifier'. Furthermore, the bank has the right not to execute the customer's payment instruction when the transaction involves "money-laundering" or any other financial crime.[288] In these circumstances the bank bears no liability for any losses to the customer.

[281] Along similar rules apply to the payee's bank liability.
[282] PSR 2009, regulation 55 (1).
[283] *Ibid.,* regulation 51 enshrines the application of Part 6 which states that the parties may agree to not apply regulations 60, 62, 63, 64, 67, 75, 76 and 77, where the customer is not a consumer, a micro-enterprise or a charity.
[284] *Ibid.*, regulation 59(1).
[285] *Ibid.*, regulation 59(1).
[286] *Ibid.*, regulation 55(1) and 55(2).
[287] *Ibid.,* regulation 67.
[288] See chapter five.

Table 3: Banks' obligations and liabilities under Part 6 of the PSR 2009.

PSR 2009	**Regulation:61** **Bank's liability for unauthorised payment transactions**	**Regulation 63:** **The payer's right to request a refund from the bank**
Liability	➢ Liability of the bank for losses from unauthorised payment transactions already executed	➢ Refund for unauthorised transactions already executed ➢ A kind of exception to the irrevocability principle of the PSR
Conditions	➢ Unauthorised transaction ➢ Notification without undue delay ➢ No fraudulent use	➢ Executed and authorised transaction ➢ Unspecified authorisation (transaction's fund) ➢ Unreasonable high found ➢ Within eight weeks from the debit date
Burden of Proof	➢ Banks ➢ Evidence of authenticated and accurately recorder transaction: regulation 60(1)	➢ Payer ➢ Provide all the requirements: regulation 63
Consequences	➢ Refund of the transaction's fund: regulation 61(a), or ➢ Restoration of the debited account of the former condition: regulation 61(b)	Refunds of the full amount of the transaction: regulation 63(1)
Request	➢ The customer denies the authorisation of the payment instruction: regulation 60(1)(a)	➢ Payer, within 8 weeks from the debit date: regulation 64(1) ➢ Provide the requirement:

	➢ The customer claims that the payment instruction executed wrongly: regulation 60(1)(b)	regulation 63(1) ➢ Re-request within 10 business days: regulation 64(5)
Limits exceptions	➢ £50 Liability of the payer until notification: regulation 62(1) ➢ payers' liability for all losses for gross negligence or fraudulent use: regulation 62(2) ➢ prescription after 13 months from the debit date: regulation 59	➢ Refund not valid for currency exchange reasons: regulation 63(4) ➢ Not valid if: (1) The payer has transmitted his consent directly to the bank: regulation 63(5)(a) (2) The payer was informed on the future transaction at least four weeks before the due date: regulation 63(5)((b) ➢ Exception for direct debits: more favorable terms for refunds are possible according to the framework contract: regulation 63(3)

According to the principles of common law, one of the main duties of the payer's bank is to employ all reasonable care and skill in the execution of the customer's EFT instruction.[289] The principles of common law apply here because, in determining the bank's liability for unauthorized EFT instructions, there are various issues involving the bank's duty to exercise care and skill which the PSR 2009 fail to clarify. The first of these is when the customer's EFT instruction is ambiguous, which raises the question of whether the bank is under a duty to execute such an instruction; the second issue is in respect of the bank's duty to exercise reasonable care and skill to prevent the facilitation of fraud. A further issue concerning the bank's duty to exercise reasonable care and skill is its liability for any losses or risk resulting from its employees' fraudulent or negligent execution during the course of their employment. Moreover, within an EFT transaction the payer's bank might employ a correspondent or intermediary bank which is considered to be an agent of the payer's bank. Thus, the issue is whether the bank will bear the liability of any risk resulting from its employment of the correspondent or intermediary bank in executing the EFT transaction or whether it is the customer's liability. Yet another issue in regard to 'the bank's duty to exercise reasonable care and skill' is its duty to adopt highly sophisticated encryption systems to protect both its own and the customers' interests. Such protection might consist of providing security and equipment sufficient to prevent any attack by hackers. The final finding is that the bank is under a duty to exercise reasonable care and skill to

[289] *Joachimson v Swiss Bank Corporation* [1921] 3 K.B. 110 at p. 127 per Atkin L.J.; *Midland Bank Ltd v Seymour* [1955] 2 Lloyds' Rep. 147 at p.168; *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 at p. 198 per Webster J; *Libyan Arab Foreign Bank v Manufacturers Hanover Trust Co (No.2)* [1989] 1Lloyd's Rep. 608; *AIB Group (UK) Plc v Henelly Properties Ltd* [2000] WL 1881366 at pp. 62-64.

execute and protect the customer's transaction.[290] These issues will now be examined.

3.4.2.1 Ambiguous EFT instructions

Problems may arise when the customer's instruction is ambiguous and the bank's transaction of the payment instruction does not accord with the payer's intention due to that ambiguity.[291] As explained above, the payer's bank is under a duty to take all reasonable care and skill in the execution of the customer's EFT instruction. Therefore, the payer's bank is obliged to adhere to the payer's EFT instruction and the bank is under no breach of its duty of care and skill if it executed the customer mandate complies with current banking practices.[292] As explained above, the customer under a duty towards his bank to prevent facilitates fraud. Therefore, the customer's order to his bank should be clear and unambiguous.[293] In *Midland Bank Ltd v Seymour,*[294] Devlin J. held that "the instruction to the agent must be clear and unambiguous".[295] Accordingly, the bank is under no breach of its duty of care and skill if it can prove that it has adopted a reasonable interpretation of the customer's ambiguous instruction.[296]

[290] Simpson, M., and Hoffmann, L., *Professional Negligence and Liability* (2012), Ch. 6.
[291] Cox, R. and Taylor, J., 'Funds Transfers', in Brindle, M. and Cox, R., (eds), *Law of Bank Payments*, (2010), p. 141.
[292] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194, at p. 205.
[293] *Ibid.*
[294] *Midland Bank Ltd v Seymour* [1955] 2 Lloyds' Rep. 147 at p.168.
[295] *Ibid.,* at p.168.
[296] *Ibid.,* at p.168.

In an EFT, the payer's bank is more concerned with security procedures to authenticate the instruction than with consent to the payment instruction. Therefore, if the payer's bank debits its customer's account on the basis of an authenticated EFT instruction that has been tested by agreed security procedures then, even if the instruction was not authorized, the bank can prove that it has exercised its duty to take reasonable care and skill in execution of the customer's mandate. Nevertheless, within common law rules, if the payer achieved to prove that the payer's bank knew or should have known that the payment order was ambiguous, the court may hold that the payer's bank is negligent and acted unreasonably if it did not ask for clarification from the payer.[297] In *European Asian Bank AG v Punjab & Sind Bank (No 2)* Goff L.J. held:

> "a party relying upon his own interpretation of the relevant document must have acted reasonably in all the circumstances in so doing. If instructions are given to an agent, it is understandable that he should expect to act on those instructions without more; but if, for example, the ambiguity is patent on the face of the document it may well be right (especially with the facilities of modern communications available to him) to have his instructions clarified by his principal, if time permits, before acting upon them."[298]

the present author's view is that due to the lack of norms for determining the EFT parties' liability in the execution of ambiguous payment instructions in the context of authenticated but unauthorized EFT instructions, there are a number of facts which ought to be considered by the courts in order to determine the bank's liability and whether it has exercised reasonable care and skill in executing an ambiguous EFT instruction, viz:

[297] *European Asian Bank AG v Punjab & Sind Bank (No 2)* [1983] 1 W.R.L. 642.
[298] *Ibid.*, at p. 656.

(A) The customer has the right to prove that the bank knew or should have known that the instruction was ambiguous; such proof may lead the court to consider the bank acted negligently in not asking the customer for clarification.[299]

(B) Cox and Taylor present three main questions which must be considered in deciding whether the bank was negligent and failed to exercise reasonable care and skill in the execution of the ambiguous payment instruction. These questions are: (1) how clear was the ambiguity? (2) Are there any communication methods available to the bank to communicate with the customer? And (3) did the bank have time to communicate with the customer before the execution of the payment instruction?[300]

These questions, however, do not address the issue of the unpredictability and uncertainty of the banks' liability for authenticated but unauthorized payment instructions. This is because this liability depends on the court's understanding as to whether the bank has acted with reasonable care or not.

3.4.2.2 The bank's duty to prevent the facilitation of fraud

The second issue in respect of the bank's duty to exercise reasonable care and skill is its duty to prevent the facilitation of fraud on occasions when it becomes aware that the customer's agent is misappropriating the customer's funds. The bank is under a duty to exercise reasonable care and skill to prevent the facilitation of fraud whenever the bank is on notice that the customer's agent is

[299] *Minories Finance v Afribank Nigeria Ltd* [1995] 1 Lloyds's Rep. 134.
[300] Cox, and Taylor, *op.cit*., p. 142.

misappropriating his principal's funds. [301] The difficulty lay in the conflict between the bank's duty to take all reasonable care and skill to prevent the facilitation of fraud and its duty to execute a payment instruction issued with the customer's mandate. [302] This duty was examined in *Barclays Bank Plc v Quincecare Ltd*,[303] where Steyn J. held that a bank must reject execution of an order if it is "put on enquiry," in the sense that the bank has a reasonable basis for believing that the order involved misappropriation of the customer's money.[304] But in this particular case, the court held that the bank's execution of the payment instruction issued from a valid and authenticated instruction, therefore no breach in the bank's duty to exercise reasonable care and skill was involved. [305] Nevertheless, in determining the bank's liability to execute authenticated but unauthorized payment instructions, each case is to be evaluated according to the particular set of facts. For example, in *Barclays Bank Plc v Quincecare Ltd* the chairman of the company fraudulently misappropriated the company's funds by ordering the company's bank by phone to transfer £344,000 from the company's bank account to the account of a firm of solicitors. The bank refused to execute the order and subsequently the chairman sent a payment order signed by his own hand. In accordance with this handwritten order, which was accepted as the customer's mandate, the bank executed the instruction. The funds were subsequently transferred from the account of the firm of solicitors to the chairman's personal bank account in the United States of America. The chairman than disappeared. The company sued the bank and

[301] *Ibid*., at p. 143.
[302] *Ibid*., at pp. 143-144.
[303] *Barclays Bank Plc v Quincecare Ltd* [1992] 4 All E.R. 363 at p. 376
[304] *Ibid.,* at p. 376.
[305] *Ibid.,* at p. 376.

claimed that the bank had made the payment in breach of its duty to exercise care and skill. In this case, the court held the bank was not in breach of its duty to exercise reasonable care and skill to prevent the facilitation of fraud, because the chairman was identified to the bank for 16 months and was thought to be trustworthy and dependable. Furthermore, the chairman notified the bank that the solicitors were the company's solicitors and the funds transfer was clarified by the fact that the company had just entered into a transaction whereby it bought four shops.[306]

Various types of criminality have emerged in connection with the growth of EFT systems. In *Shah v HSBC Private Bank (UK) Ltd,*[307] the court held that if the bank suspects that the customer's transaction involved money laundering as defined in the Proceeds of Crime Act 2002, the bank has the right not to execute the payment transaction without having to demonstrate that there are reasonable grounds for such a suspicion.[308] The bank is only under a duty to exercise reasonable care and skill to execute its customer's EFT instruction if such execution will not place it in breach of legal provisions.[309]

The author's view takes account of the fact that in the EFT transactions the bank receives the instruction electronically and so a massive number of instructions need to be executed in nearly-real time. Thus, the bank has no capacity for determining whether an EFT instruction issued from the rightful customer or whether there is misappropriation of the payer's funds, and at the same time the bank is more concerned with the authentication of the instruction

[306] *Ibid.*
[307] *Shah v HSBC Private Bank (UK) Ltd* [2013] Bus. L.R. D38.
[308] *Shah v HSBC Private Bank (UK) Ltd* [2009] EWHC 79 (QB) at paras. 23 and 60.
[309] See chapter five.

than with its consent. Therefore reasonable to consider the bank not liable for the execution of payment instructions issued on behalf of the customer or for the misappropriation of the payer's funds, as long as the execution of such instructions depended on the use of the agreed authentication procedures. However, the customer will have the right to sue the person who acted on his behalf or who misappropriated his funds on the basis of the contractual relationship between them. Finally, the question of whether the bank has exercised its duty of care and skill is open to interpretation on the part of the court.

As explained previously, the customer is under a narrow duty to exercise reasonable care and skill to not facilitate fraud. Indeed, the customer is under a duty to protect and save the physical card but not the card data, for example, the card number and PIN. An offender can obtain the card data very easily, and it is not reasonable to consider a customer is liable when an offender copies such data when the customer is undertaking a perfectly lawful transaction, such as using the card in a supermarket, café shop or restaurant.

Furthermore, when the customer makes a transaction over the telephone or on the internet, he must provide the card holder name, number of the card and the three digit security number. The purpose of security number is to prove and confirm that the card is in the possession of the customer, assuming that only the customer who must know such number.[310] But if the third party obtains of a photocopy of the card without the knowledge of the customer, the third party will be in possession of all the card data, and if the third party then uses the card

[310] Mason, *op. cit*., p. 40.

over the internet, there is no proof that the person conducting the transaction is the customer himself or the third party.[311] In this regard, in *Halifax Union v Wheelwright*,[312] Baron Cleasby held:

> "a man cannot take advantage of his own wrong, a man cannot complain of the consequence of his own default, against a person who was misled by that default without any fault of his own."[313]

Mason believes that such comment has a reverberation to the modern world of electronic banking as ever it did when Baron Cleasby wrote it.[314] Such comment means that when the bank decides to use an encryption system that is insufficient by secure, then the bank must bear the liability.[315] The bank cannot obtain benefit of the flaw in the machinery that customers are required to use, such as: the flows of data through a number of third parties; the failure of employees that are liable for the machinery; and the failure to fully control the complex sub-contracting that takes place within the industry. [316] The bank cannot complain of the consequences of their own default against customers who are misled by those very defaults of technology and the failure to obey operating manuals. [317] Given the above position, it seems that it is reasonable to consider the bank liable for authentication but unauthorised transaction when the customer denies issuing such transaction and there is no fraud or negligence on the part of the customer.

---

[311] *Ibid.*
[312] *Halifax Union v Wheelwright* (1874-75) L.R. Ex. 183 at p. 192.
[313] *Ibid.,* at p.192.
[314] Mason, *op. cit*., p. 40.
[315] *Ibid*.
[316] *Ibid*.
[317] *Ibid*.

3.4.2.3 The bank's liability for its employees and agents

EFT is significantly vulnerable to fraud by employees.[318] The bank is liable for any losses or risk resulting from its employees' fraudulent or negligent execution during the course of their employment.[319] In the case of an EFT payment initiated by the fraud of a bank employee, the customer whose account was debited as a result of the fraudulent instruction has the right to instruct the bank to re-credit his account, because the bank's action was without the customer's mandate.[320] An example of employee fraud would be when the bank employee changes the customer's address, issues a new payment instrument and sends it to the new address, then later uses the payment instrument to withdraw funds from the customer's account,[321] this exactly what happened to Emma Woolf, who discovered that £10,000 had been withdrawn from her business account with Abbey, a bank later taken over by Santander.[322] The bank denied that it was culpable on the grounds that everything involved in the transactions, including the payment instrument and security procedures used, was legal. Subsequently, Thames Valley Police visited the home of one of the bank's employees as part of an inquiry unconnected with Emma Woolf's case. During their inspection of the premises the police found many documents pertaining to Ms Woolf's bank account, include the missing payment instrument and bank statements. The employee was arrested because another customer had had £150,000 withdrawn from his account in the same way. The fraud was

[318] *Ibid.,* at p.16.
[319] Wadsly and Penn, *op.cit*., p. 374; Cox and Taylor, *op.cit*., p. 181.
[320] Cox, and Taylor, *op.cit*., p. 181.
[321] Mason, *op. cit.,* p.16.
[322] This example has been given by Mason, see *Ibid.*

committed by means of changing the address of the customers' accounts, sending new payment instruments to the new addresses, obtaining the PIN from customers' records and then withdrawing the funds from ATMs. Santander denied its liability, although it took settlement procedures as follows: first, repayment the funds withdrawn from both customers' accounts; secondly, payment all the legal fees involved; and thirdly, as part of a settlement the customers signed a privacy agreement, the terms of which allowed the bank to avoid either apologising to the two customers or offering them any reimbursement.[323]

There is no particular evidence of authentication procedures being subject to attack, that is because yet there is no published evidence that a chip and PIN cards are subjected to cloned.[324] Although, recently, Bond[325] develops a new methodology to proof the card is cloning. Bond states:

> "This protocol requires point-of-sale (POS) terminals or ATMs to generate a nonce, called the unpredictable number, for each transaction to ensure it is fresh. We have discovered that some EMV (Chip and PIN) implementers have merely used counters, timestamps or home-grown algorithms to supply this number. This exposes them to a "pre-play" attack which is indistinguishable from card cloning from the standpoint of the logs available to the card-issuing bank, and can be carried out even if it is impossible to clone a card physically."[326]

Accordingly the customer can present evidence to prove that his card is cloned and pursue the bank for a refund.[327] There is no doubt that, if security procedures were cloned, the bank would be liable for any losses. Thus the

[323] *Ibid.*
[324] Mason, *op. cit.,* p.58
[325] Bond, M., et al., 'Chip and Skim: cloning EMV cards with the pre-play attack', (2012) *arXiv preprint arXiv:1209.2531* 1 at p. 1 http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf 15 March 2013.
[326] Bond, *op.cit*., p. 1.
[327] *Ibid.,* at p. 2.

banks, eager to minimize their liability for unauthorized transactions, offer no means for determining whether there is cloning of security procedures.[328] Within the PSR 2009, where the customer denies authorizing the instruction it is the bank's responsibility to prove the converse.

In an EFT transacting, the payer's bank might employ a correspondent or intermediary bank which is considered to be an agent of the payer's bank.[329] Within common law rules it is the payer's bank which bears the liability for any failure, fraud or negligence of the correspondent or intermediary bank in executing the EFT transaction, as the correspondent or intermediary bank is the payer's bank's agent.[330] This is acceptable because it is held that there is no contractual agreement between the customer and the intermediary bank and thus the intermediary bank owes no liability to the payer. In *Royal Products v Midland Bank*[331] Webster J. held that when the bank adopted an intermediary bank there are two contracts, the first between the payer's bank and its customer and the second between the payer's bank and the intermediary, and that both fell within agency law with regard to EFT. Thus, the payer's bank owed to the customer and the intermediary bank owed to the payer's bank a duty to exercise reasonable care and skill.[332] The payer's bank was therefore liable to the customer for non-execution of the payment instruction by its agent. The intermediary bank, however, had no duty of care and skill towards the customer because there was no contract between them. On this point, Webster J. held:

---

[328] *Ibid.*
[329] Ellinger, *op.cit.,* p.617; Wadsly and Penn, *op.cit*., p. 374; Cox, and Taylor, *op.cit*., p. 146; Further, see chapter four of this thesis.
[330] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194.
[331] *Ibid.,* at p. 198.
[332] *Ibid.*

> "in carrying out its part of the transaction Midland (payer's bank) owed Royal (the payer) a duty to use reasonable care and skill…and that they would be vicariously liable for the breach of that duty by any servant or agent to whom they delegated the carrying out of the instructions. Midland, therefore, would be liable to Royal Products for National's (intermediary bank) negligence, if any, in that respect. But in my judgment National owed no duty of any kind direct to Royal Products. …In my judgment, therefore, National are not to be regarded as having been agents of Royal Products and did not, therefore, owe them any of the duties, including a fiduciary duty, owed by an agent to his principal"[333]

In modern banking practice it has become normal for the banker-customer contract to include an express term excluding liability for any default or negligence on the part of the intermediary bank.[334] Accordingly, in the case of the intermediary bank's non-execution of a payment instruction, the customer has no right under any circumstances to claim or request a refund from the payer's bank because of the exclusion terms. In turn, the intermediary bank has no liability towards the customer due to the absence of a contractual relationship between them. However, although there is no contractual liability the issue is whether the customer could sue or make a claim to the intermediary bank for any loses caused by it, depending on tort liability. In *Calico Printers Association v Barclays Bank Ltd,*[335] the claimant ordered Barclays to insure certain goods. However, Barclays' correspondent bank in Beirut failed to do so. The claimant pursued both Barclays and the correspondent bank.[336] Wright J. held that there was no contractual relationship between the intermediary or correspondent bank and the customer, and thus there is no contractual liability even if the intermediary bank is nominated in the contract between the customer and the payer's bank since such nomination creates no privity of

[333] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 at p.198.
[334] *Calico Printers Association v Barclays Bank Ltd* (1931) 39 Lloyds List Rep. 51.
[335] *Ibid.,* per Wright J.
[336] *Ibid.*

contract between the customer and the intermediary bank.[337] His Lordship dismissed the claim against the correspondent bank under reason that there was no privity of contract between the claimant, customer, and the correspondent bank.[338] In the absence of contractual liability between the customer and the intermediary bank (sub-agent), can the customer sue the intermediary bank according to a duty of care in tort at common law? In *Calico Printers Association v Barclays Bank Ltd,* Wright J. held that as a general rule the payer has no right against the correspondent bank, as sub-agent for negligence or breach of obligation.[339] General rules are that a sub-agent owed no a duty of care to customers in the EFT,[340] since the ambit of such duty depends heavily on the direct communications between the customer and sub-agent which are unlikely to arise in an EFT transactions.[341] Thus no tort liability exists between them. In this respect the intermediary bank has no duty of care whatsoever to the customer.[342] Since the customer cannot sue the sub-agent in contract or tort it would appear that the bank (agent) remains liable for the defaults of the sub-agent.[343] Nevertheless, the exclusion of liability could be subject to an evaluation under the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contracts Regulations 1999.[344] Where the payer is involved in the funds transfer in a business capacity, it is upheld within the

[337] *Ibid.*, at p.80; *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194, at p.198 per Webster J.; Further, in *Grosvenor Casinos Ltd v National Bank of Abu Dhabi* [2008] 1 C.L.C. 399 at [175], Flaux J. held that in the EFT the receiving bank in Abu Dhabi was under no duty of care to the payee in tort where the payee's bank in the UK had sent the cheque for the aim of receipt
[338] *Calico Printers Association Ltd v Barclays Bank Ltd* (1931) 39 Lloyds List Rep. 51.
[339] *Ibid.*
[340] *Balsamo v Medici* [1984] 1 W.L.R. 951 at pp. 959-960
[341] *BP Plc v AON Ltd (No. 2)* [2006] 1 C.L.C. 881.
[342] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194, at p.198 per Webster J.
[343] Markesinis and Munday, *op.cit.,* p. 101.
[344] Unfair Terms in Consumer Contracts Regulations 1999 (SI 1999/2083).

Unfair Contract Terms Act 1977[345] that the banks have the right to include their contracts with the customers term to exclude liability, but only if this term is deemed reasonable. In practise, with regard to business customers such exclusion is considered acceptable and reasonable, and the paying bank bears no liability for the correspondent or intermediary bank's negligence. This interpretation is based on the view that the payer's bank has no control with regard to its agent's actions, and that a business customer expects and accepts this and insures against the risk. Conversely, it is held that a payer who is involved in the funds transfer as a customer has the opportunity to depend on both the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contracts Regulations1999, [346] because both statutes cover all contractual terms that have been not subject to the negotiation.[347] Within these statutes, if the contract includes an 'unfair' term the customer shall not be liable for non-execution of that term. As long as the payer's bank is under a duty to exercise reasonable care and skill and has selected the intermediary bank as its agent it is reasonable to consider the exclusion of the bank from liability as 'unfair'. However, it is difficult for the customer to establish the claim that his bank failed in its duty to exercise reasonable care and skill in selecting the intermediary bank, particularly when the intermediary bank is a reputable one.

Within the PSR 2009 the position is different. The payer's bank is liable to the payer until the transactions funds are actually credited to the payee's

[345] Unfair Contract Terms Act 1977, Schedule 2.
[346] *George Mitchell (Chesterhall) Ltd v Finney Lock Seeds Ltd* [1983] 2 A.C. 803; Peel, E., *The Law of Contract* (2007), para. 7-017.
[347] Unfair Terms in Consumer Contracts Regulations1999, regulation 3(1).

account.[348] Thus, it seems that where the customer is a consumer there is no opportunity for the payer's bank to avoid its liability for any defaults or negligence on the part of the intermediary bank. While in the case of business customers the bank can avoid such liability if there is an existing agreement between the parties for not applying the regulation.[349] If the payer's bank failed to make the payment, the payer has the right to claim against his bank,[350] and the payer's bank in turn has the right to claim against the intermediary bank.[351] Furthermore, both the payer and the payer's bank have the right to claim under tort liability. It makes no difference whether or not the payer is a customer of the bank: within the PSR 2009 the payer's bank owes a duty to exercise all reasonable care and skill both to the customer of the payer's bank and to the payer who is not a customer.[352] Under common law rules such a duty arises from the contractual agreement between the customer and the bank and the bank is also under a duty in tort.[353] The payer's bank has no duty of care to the payee,[354] either under contract liability or tort liability,[355] except when the payee has an account in the same bank as the payer.[356]

[348] PSR 2009, regulations 70 and 75.
[349] *Ibid.*, regulation 51 (3)(a).
[350] *Ibid.*, regulation 120.
[351] *Ibid.* regulation 78.
[352] *Ibid.*, regulations 33 and 51; Supply of Goods and Services Act 1982, section 13.
[353] Further details, see chapter six.
[354] Cox, and Taylor, *op.cit*., pp. 150-152.
[355] *Wells v First National Commercial Bank* [1998] P.N.L.R. 552 at pp. 557-560.
[356] *Laemthong International Lines Co Ltd v Artis* [2005] EWCA Civ 519; *Prudential Assurance Co. Ltd v Ayres* [2008] EWCA Civ 52.

3.4.2.4 The bank's liability for adopting adequate security systems

Regarding the bank's duty to exercise reasonable care and skill, banks must adopt sufficient encryption systems to protect both its own and its customers' money also to prevent unauthorized access to the customers' accounts by providing security and equipment sufficient to prevent fraud. The bank is under strict liability to employ reasonable and secure software programs for executing its intended purposes and such liability does not depend on proof that the bank was negligent.[357] If such liability is not expressed by a term in the contract there will be an implied term under the common law rules stipulating that the system is required to be capable of achieving its intended purpose.[358] Furthermore, within PSR 2009 it is the bank's liability to prove that the customer instruction was accurately executed and not affected by a technical breakdown or other security problems.[359] Thus, the bank will be liable to the customer for any defaults or inadequate in the security system employed by the bank to protect and pass the funds transfer. A question which arises is: who should bear the risk for unauthorized transactions when neither the customer nor the bank has acted negligently? A second question is: who should bear the risk for unauthorized transactions when both the customer and the bank have acted negligently? The answer could be found in the Regulations 2009: the customer who acted without gross negligence or fraudulence bears no liability unless he is not apply the Regulations 2009 requirements here bears up to £50 for any

[357] *St Albans City and DC v International Computers Ltd* [1997] F.S.R. 251.
[358] Cox, and Taylor, *op.cit*., pp. 145-146.
[359] PSR 2009, regulation 60.

losses resulting from unauthorized transactions.[360] However, if EFT transactions fall outside the ambit of the PSR 2009, the question of determining liability when both the customer and the bank are negligent or neither of them is negligent is unpredictable and uncertain.[361] The author's view is that when both the customer and the bank are negligent or neither of them is negligent than the bank is liable to bear the risk of unauthorized transactions, because one of the bank's duties to the customer is to exercise reasonable care and skill to execute the customer's transaction, while the customer is not obliged to exercise reasonable care and skill, unless such duty is specified in the banker-customer contract. Even more, the author's view is the bank is obliged to provide sufficient security system and thus an offender who obtains the customer's security procedures, such as PIN and card data, without the knowledge of the customer, the bank is liable for any losses resulting from using the card by the offender, and it is the bank liability for authentication but unauthorised transaction. The bank bears the losses because such authenticated but unauthorized transaction accrued as a result of the technology that the bank makes its customers use. The customer bears no liability for failing to deal with such risks, because these are risks under the control of the bank. The bank wishes to challenge the customer association with a transaction was unauthorized, it must prove that the customer used the agreed security procedure and the legal payment instrument, and that there was no inadequacy in the software programs.

[360] *Ibid.,* regulation 62(2).
[361] Geva, *Bank Collections and Payment Transactions*, *op.cit.,* p. 398.

Indeed, both the banks and the customers' liability for unauthorized transactions are uncertain and unpredictable in the context of EFT unauthorized transactions. Therefore, there is a need to regulate the EFT parties' liability to make them more certain and predictable would mark a significant improvement. Any such regulation, however, should take into account the uncertainties cited above.

3.4.2.5 Banking practice in guarding against unauthorized EFT transactions

Because internet systems are available to all users fake websites designed to capture card information are outside the control of the bank. This poses the question of how card issuers such as Visa and MasterCard actually guard against fraud and how they protect themselves.

Visa and MasterCard have established different types of safeguard to protect both themselves and their customers from unauthorized use of payment instruments. First, banks request the customer to refrain from providing bank account information by email. If a bank customer receives an email claiming to come from the bank and requesting account information, the customer should never provide such information without contacting the bank to enquire whether the email was genuine. Visa provides an email address through which the customer can contact them for further investigation.[362] A second safeguard

[362] http://www.visa.co.uk/en/security/online_security/online_fraud.aspx 6 September 2012.

intended to protect customers from online fraud is 'Verified by Visa.'[363] This operates by issuing the customer with a 'Verified by Visa' password which is known only to the customer. The online procedure for 'Verified by Visa' is the same, no matter which bank issued the card.

A third and significant safeguard against fraud provided by the issuers is in the form of "chargeback". "Chargeback" is a procedure whereby a card issuer charges the funds transaction back to the merchant acquirer in accordance with a contractual relationship between the card issuer and the merchant. It is the issuer's right to request from the merchant a 'chargeback' for invalid transactions according to the contractual agreement between them.[364] The question thereby arises of whether there is any legal issue regarding such schemes. Within section 75 of CCA 1974, if a customer pays with a credit card only and subsequently disputes a transaction against the seller, the card issuer has the right to request a refund. However, section 75 covers only transactions from £100 up to £30,000. The Court of Appeal in *Office of Fair Trading v Lloyds TSB Bank Plc*[365] held that section 75 applies to credit card schemes regardless of the number of parties, which may be three or four when a merchant acquirer, is involved, and regardless of whether the transaction takes place in the UK or abroad. Section 75 applies when there is misrepresentation or breach in credit card schemes. There is no regulatory protection which applies to debit card transactions. However, as explained above, according to the PSR 2009 the

[363] http://www.visa.co.uk/en/security/online_security/verified_by_visa.aspx 6 September 2012.
[364] The National Archives, Department for Business Innovation and Skill http://webarchive.nationalarchives.govuk/+/http://www.bis.govuk/policies/consumer-issues/buying-and-selling/prepayments 6 September 2012.
[365] *Office of Fair Trading v Lloyds TSB Bank Plc* [2006] 3 W.L.R. 452 at p. 453.

cardholder has the right to request refunds for unauthorized transactions.[366] In practice, chargeback is deemed to be part of Visa and Master card's internal principles. Visa's chargeback is not limited by the value of the transaction, but MasterCard's chargeback is limited to a minimum of £10. The cardholder must request chargeback for the disputed transactions' funds within 120 days of recognising a problem.[367]

Finally, the common safeguard used by banks against fraud and preventing unauthorized transactions is to include another form of communication between the bank and the customer, for example, a text message or telephone call. When a customer issues a fund transfer order, the bank will send a text message to the customer's mobile telephone, requesting them to enter an authorization code in the browser that is provided in the text message. This kind of guard does not provide the customer with sufficient protection against the offenders, because this process does not prevent the offenders from circumventing the security. Such circumventing could be accrued when the offender persuades the customer telephone company to supply him with an extra SIM card so he can use the customer telephone, possibly by claiming that the SIM card has failed, so the offender can impersonate the customer mobile telephone. Another flaws with this method of protection is not all the bank's customer has mobile telephone, thus this method cannot consider sufficient to protect the customer from unauthorized transaction.

[366] PSR 2009, regulation 63.
[367] www.visa.com 6 September 2012.

3.5 Conclusion

The existing law of EFT systems locates some of the risk for unauthorized payment with the bank. The conclusion drawn in this chapter is that the parties' obligation to take reasonable steps of care and skill in the issue and execution of EFT instructions occupies an important role in determining the liability for unauthorized EFT. Nevertheless, such an obligation to determine the parties' liability has led to uncertainty and unpredictability. The uncertainty of liability exists due to the rules governing cheque forgery being inappropriately applied to EFT fraud. The payment instruction for a cheque is issued and authenticated by means of the holder's handwritten signature, whereas an EFT instruction is issued electronically and authenticated by security procedures. In this respect, the customer is in more control of writing out a cheque, but the crucial difference between the cheque and the card and the PIN is that the card and PIN can only be considered to be in the relative safe keeping of the customer, and when the card is used, it is exposed to the weaknesses of the technology. For these reasons it is difficult for the bank to identify the person who used the security procedures and to ascertain whether he is the authorized person. Finally, an examination and evaluation of the rules of agency law and contract law which are applied to unauthorized transactions in the EFT context fails to provide sufficient determination of the parties' liabilities in unauthorized EFT instructions.

PSR 2009 imposes on the bank obligations and liabilities to protect the customer in cases of unauthorized EFT payments. The payer's consent to the execution of an EFT instruction can be either express or implicit. Nevertheless,

PSR 2009 involves authorization of payment instruction only if there is express consent from the payer. The conclusion reached in this chapter is that the PSR 2009 is unhelpful in defining those situations where the customer might be taken implicitly to have authorized a transaction. The author's view is that the existing laws, regimes and private card network principles provide an insufficient number of incentives to both customers and banks for adopting practices which would reduce the incidence of unauthorized EFT. It seems therefore that in the context of EFT that the focus of the approach ought to be more comprehensive and take the form of a Consumer EFT Act which would determine the liability of all parties involved in an unauthorized payment instruction. Finally, this chapter argues that the bank is under a duty to exercise reasonable care and skill towards its customer, while the customer under no such duty. Regarding to the bank's duty of care and skill, it is the bank liability for authentication but unauthorised transaction.

Chapter Four

EFT Parties' Liability for Insolvency Risk

4.1 Introduction

With regard to EFT payment, 'completion of payment' can have more than one meaning. Firstly, it means that the payer loses the right to cancel or revoke the payment instruction, principally in cases of insolvency. Secondly, it means the point at which the payee's bank has the liability to credit the payee's account. This chapter focuses on these two meanings. It is concentrated on determining which party bears the risk of EFT non-payment. Addressing the exact time of completion of EFT payments between the payer and the payee is helpful in identifying the party which bears the risk of non-payment. Further, the legal nature of the payment, namely, whether it is conditional or absolute, is treated as a significant issue in relation to the finality of the EFT. This chapter will therefore deal first with the completion of EFT payment between the payer and the payee. Secondly, it will examine the legal nature of payment. Finally this chapter will determine which of the parties bears the risk of insolvency in the EFT context.

The completion of EFT payment is a significant factor in the systemic stability of payment systems. It defines the liability of the final destination bank, the point at which the EFT is considered to be final and cannot be reversed under any circumstances, such as default or insolvency of the participating parties. In a

debit transfer the payer's bank is liable, while, conversely, in a credit transfer the payee's bank is liable.[1] The absence of particular rules in locating precisely the time of payment completion in the context of EFT exposes the transactions' parties to unpredictable and ambiguous liability for non EFT payment. Thevenoz confirms:

> "The absence of a well-defined body of law applicable specifically to paperless funds transfer, both in Common Law and in several Civil Law countries, has created much uncertainty, especially with regard to the finality and revocability of a payment order,…, error and insolvency. These uncertainties became a major concern to banks experiencing the lack of a statutory ''safety net'' as soon as some of their largest clients refused to accept disputed contractual provisions allocating losses."[2]

This chapter analyses current rules and suggests recommendations for the future of EFT regulation. Different rules and principles for determining the exact time of payment completion will be assessed, and the comparable and conflicting points will be analysed. Finally, an attempt will be made to formulate appropriate rules in order to address the deficiencies in the current regulations.[3] Identifying the time of EFT completion assists in demonstrating which of the parties bears the risk of non-payment in the context of EFT. This chapter discusses applicable provisions of the PSR 2009 in dealing with the time when the transaction's funds must be delivered to the payee. Furthermore, it investigates the issues involved in both debit and credit transfers, and focuses on the principles of contract and agency law by analysing those rules. This chapter advocates the regulation EFT payment completion in one body of law, covering the liability of parties involved in EFT transactions, and duties and

[1] Geva, B., 'Payment finality and discharge in funds transfers', (2008) 83 *Chicago-Kent Law Review* 633 at p. 634.
[2] Thevenoz, L., 'Error and fraud in wholesale funds transfers: U.C.C. Article 4A and the UNCITRAL harmonization process', (1991) 42 *Ala. Law Review* 881 at p. 883.
[3] See chapter seven, section 7.3.

obligations in case of non-payment. Section 4.2 will investigate the provisions of the PSR 2009, beginning with the execution of payment transactions. It then argues that the PSR 2009 do not address the exactly time when the EFT becomes final. Although the PSR 2009 establishes clearly that the funds have to be available to the payee before the payment is considered final, it fails to provide the exact definition of availability in relation to funds. Section 4.3 of this chapter is dedicated to analysing the common law rules. This section summarizes the arguments favouring the establishment of basic rules governing the finality of EFT in order to identify which of the parties bear the risk of non-payment. It argues that the EFT should be final at the destination bank in the system chain.

4.2 Execution of EFT instructions under the PSR 2009

Regulations 65-79 of the PSR 2009 set out instructions for the execution of payment transactions without presenting any definition of the term ‘execution’. The term ‘execution’ refers to the completion of the payment transaction and not to the execution of the instruction delimited in the EFT transaction. Elsewhere in the Regulations 2009, however, the term execution is used to refer to the execution of payment instructions.[4] Use of the term ‘execution’ within the PSR 2009 is therefore inconsistent and the Regulations need to be amended in this respect.

[4] For instance, PSR 2009, regulation 66 applies in case of refusal of payments orders.

Part 6 of the PSR 2009 governs the execution of payment orders and funds transferred; both sent and received,[5] execution time and value date,[6] and finally liability.[7]

4.2.1 Execution of EFT payment instructions

PSR 2009 deals with the receipt, refusal, or revocation of payment instructions.[8] The payer's bank has to execute the payer's instruction once it is received. The different time-limits are generally considered from the 'time of receipt', which is the time at which the payer's bank receives the order to execute the fund transfer transmitted to the payer's bank either by the payer directly, as in a credit transfer; by the payer indirectly via the payee's bank, as in a debit transfer; or indirectly by or via the payee, as in a direct debit.[9] If the payer and his bank agree a specific time to make the payment then the 'time of receipt' will be taken as the agreed time, for example, for a standing order.[10] In both cases, the 'time of receipt' will be the next business day if it is received on a holiday.[11] Furthermore, the payer's bank has the right to set a deadline so that the 'time of receipt' is the next working day for orders received after that time.[12] It is compulsory for the paying bank to carry out the payer's order within the time-

[5] PSR 2009, regulations 65-68.
[6] *Ibid.*, regulations 69-73.
[7] *Ibid.*, regulations 74-79.
[8] *Ibid.*, regulations 65-68.
[9] *Ibid.*, regulation 65(1).
[10] *Ibid.,* regulation 65(4); Regulation 70(4) set out one limitation to such freedom: 'where the payment order is to be carry out within the EEA, the paying bank must be certain that the funds of transaction is available to the payee's bank by the end of the fourth business day after the 'time of receipt' of the payment order'.
[11] *Ibid*., regulations 65(2) and 65(5).
[12] *Ibid*., regulations 65(3).

limits set out in the PSR 2009, where it is applicable.[13] Although, where the payer's order is originally given by paper-based means, rather than electronic means such as over the telephone or internet, a different rule applies. In such case the payer's bank must ensure that the payee's bank account is credited by the end of the next day following the 'time of receipt' of the payer's order.[14] Even where these different time-limits explained above do not have compulsory application; the paying bank and the payer however may agree that they shall apply.[15] The payer and his bank are free to agree that some other specific time should apply to their payment instruction, but there is one limit upon that freedom: where a payment instruction is to be completely carried out within the EEA, the paying bank must be certain that the funds of transaction is available to the payee's bank by the end of the fourth business day after the 'time of receipt' of the payment order.[16]

The payer has the right to withdraw his consent to the transaction,[17] but as a general rule he has no right to cancel the payment instruction once it has been delivered to the payer's bank.[18] A different rule applies to the cancelation of payment instructions for direct debits, as the payer may not cancel his instruction after the end of the working day preceding the day agreed for the debiting of the funds.[19] In other cases where the payment instruction is initiated by or through the payee, it is completed once it is either communicated, or

[13] *Ibid*., regulation 69(1).
[14] *Ibid*., regulation 70(3)(a) and 70(3)(b).
[15] *Ibid*., regulation 69(2).
[16] *Ibid*., regulation 70(4).
[17] *Ibid*., regulations 55(3).
[18] *Ibid*., regulations 65(1) and 67(1). Taking into consideration regulation 51 (3)(a) which provides that where the customer is a business the parties have the right to agree not apply regulation 67.
[19] *Ibid*., regulations 67(3).

transmitted, or the payer's approval is given;[20] it is equivalent to prior authorization introduced by the payer to the payee to create the debit transfer instruction. Thus, for example, the payer has no right to cancel the payment instruction after inserting the PIN on a card transaction. Where there is an agreement between the payer and the payer's bank that the payment instruction is to be carried out on a specific day, for example, the day when the payer credits his account, or on the last day of a certain period, for example, a standing order, the payer loss his right for cancelation the payment after the end of the working day preceding the agreed day of payment.[21] However, and regardless of the transaction type, whether it is a consumer or business transaction, the payer has the right to cancel a payment order outside the different time-limits recognised by the PSR 2009 only if he obtains his bank's approval to such cancelation.[22] When the payment instruction is initiated by the payee such as direct debits, the payer must also obtain the payee's approval before the payment order can be cancelled out of time.[23] Where the payer cancels a payment order that is initiated according to the terms in the contract with his bank, the bank may charge the customer for revocation[24] if it is stipulated in their agreement and must reasonably correspond to the actual costs incurred by the payer's bank.[25]

The general principle is that the payee's bank must accept the payment instruction. While the PSR 2009 carries no reference to any such compulsory

[20] *Ibid.*, regulation 67(2).
[21] *Ibid.*, regulation 67(4).
[22] *Ibid.*, regulation 67(5)(a).
[23] *Ibid.*, regulation 67(5)(b).
[24] *Ibid.*, regulation 67(6).
[25] *Ibid.*, regulation 54(1). Taking into consideration regulation 51 (3)(a) which where the customer is a business the parties has the right to agree not apply regulation 54(1).

acceptance, it seems that receipt and acceptance of a payment instruction by the payee's bank for the benefit of the payer's payment instruction refers to the finality of funds transfer. Therefore, the author's view is that acceptance by the payee's bank of the payment order indicates the finality of the EFT. Moreover, acceptance of the payment order by the payee's bank refers to the payment by the payer to the payee, in this sense, liberating the payer from obligation on the underlying transaction of the debt charged by the EFT. Thereby, the payee's bank is liable to pay the transaction's funds to the payee. Basically, the payment is considered to be made when the payee's bank has credited the payee's account and no condition or provision is placed on the receiver's funds.

Although, the Regulations 2009 contain no reference to rules governing the acceptance of a payment order from the payee's bank, they do address the rules dealing with refusal of payment orders. These grant the bank no absolute right to refuse execution of the payment order and include an obligation on the part of the bank to notify its customer of reasons for the refusal and of the method for enabling any possible refund.[26] Accordingly, if the payment instruction is issued properly, applying all the agreement's requirements, and there is no lawful reason for non-execution, then the bank has no right not to execute it.[27]

[26] *Ibid*., regulation 66(1).
[27] *Ibid.*, regulation 66(5).

4.2.2 Execution time and value date of EFT transactions

The term 'execution' refers to the finality of a payment instruction, either by crediting the funds transfer in the payee's bank account or by crediting the payee's account.[28] In this sense, as long as the time of crediting the payee's bank with the transaction is the time when the payment is to be considered final, it is not clear why crediting the funds in the payee's account is essential to considering the payment final. It might be considered that finality of payment occurs when the payer's account is debited by his bank. As explained above, Regulations 2009 require that the funds transfer must be credited to the payee's account by the end of the working day following the time of receipt of the payment instruction.[29] However, the Regulations offer no definition of what is meant by 'funds availability'. As a general term, 'funds availability' must refer to the absolute use of the transactions' funds by the payee, as with cash. The authors' view is that 'funds availability' does not have to be equivalent to cash for the payment to be considered final. It is sufficient that the funds are credited to the payee's bank account. Therefore, if the payee's bank account is credited with the transactions' funds, and at the same time his account was overdrawn, the bank has the right to deduct the overdraft funds from the transaction's funds and the payment is considered to be final, despite not being available to the payee in the same way as cash.[30]

---

[28] *Ibid.,* regulation 70.
[29] *Ibid.,* regulations 73, this regulation apply to payment discharged by the currency of any other EU member States.
[30] For example, Lloyds TSB, Personal Banking terms and conditions, October 2012, section C[10.3], [10.4]
http://www.lloydstsb.com/media/lloydstsb2004/pdfs/personal_banking_terms_and_conditions.pd

The PSR 2009 obliges the payer's bank to ensure that the transaction funds are credited to the payee's bank account by the end of the working day following the day the payment instruction was received.[31] However, there is no remedy for the payee in the case of breach by the payer's bank, such as a delay in executing the transfer. It appears that the only available remedy would be the payee's right to sue the payer, and in turn the payer claiming reimbursement from his bank. The payee's right against his bank is established in case of a default on the part of the payee's bank after having received the funds from the payer's bank. The payee's right is indicated to be the actual time of crediting the payee's account. In addition, the payee's bank must guarantee that the funds for the transaction are in the payee's account once the amount has been credited to the payee's bank. This period of time is applicable whether the payee is a customer of the bank or not.[32] Notwithstanding these provisions the payee is still without any remedy for a delay in funds credited to the account of his bank in breach of this rule.[33] Credit value for the payee's account must not be delayed more than one working day following the time of receipt of the payment instruction. The author's view is that to stipulate that the funds transaction must be credited in the payee's account by the end of next business day is to create the possibility of a number of issues which banks will need to address The first issue arises when the EFT transaction involves merchant acquirers.

---

f; HSBC, General Terms and Conditions, Current Accounts Terms and Conditions, April 2012, section 4 http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf 6 October 2012; Further details about overdraft facility see section 4.4.2.

[31] PSR 2009, regulation 70(1).

[32] *Ibid.,* regulation 70.

[33] Geva, B., 'Payment transactions under the EU payment services directive: A U.S. comparative perspective', (2009) 27 *Penn State International Law Review* 713 at p.727.

A hypothetical case might involve merchant acquirers holding different payment accounts on behalf of their merchant customers. Here the execution of the provision of credit value for the payee's account where no delay is involved should not create any issue. This is because when a payment instruction executes, the merchant acquirer will request the funds from the payer's account. The funds must cross the merchant acquirer's account for the merchant the following day. Consequently, the merchant acquirer orders a payment for the account it keeps on behalf of the merchant to the merchant's bank account. In such transactions the fund must cross the merchant's account on the day following day one.[34]

The second hypothesis, however, is that the merchant acquirers do not hold accounts on behalf of the merchant. There are a number of issues for the merchant acquirer to overcome in order to ensure that the transaction fund credits the payee's account on behalf of the merchant receipts by the merchant's bank account at the end of the business day.[35] The author agrees with Brandt and Graham's view that there is no doubt that the first approach is preferred because it achieves the aims of Regulations 2009 as well as reducing disruption to the payment services market. The second approach, involving the claim that merchant acquirers do not operate accounts on behalf of merchants, depends on the argument that the merchant acquirers passed payments to the merchants before they had credited the funds from the payee. However, such an argument has been rebutted on the following grounds: that the merchant acquirers passed payments to merchants before they had credited the funds

[34] Brandt, P. and Graham, P., 'An update on the UK's implementation of the Payment Services Directive', (2009) 64 *Compliance Officer Bulletin* 1 at p.27.
[35] *Ibid.*

from the payee does not mean that the merchant acquirer did not hold an account on behalf of the merchant.[36] It means that the account operated by the merchant acquirer on behalf of the merchant had a debit balance until the payee transferred the funds and the account was credited with the transaction fund.

The second issue concerns internal payment transactions. Indeed, it is difficult for the bank to ensure that the transactions funds are credited in the payee's account at the end of business day, particularly when the payer and the payee have accounts in different banks. Finally, the provision that the funds transaction must be credited in the payee's account by the end of the next business day leaves the payer without the right to revoke the payment instruction as long as the payment is passed once the instruction is issued.

4.2.3 Liability for non-execution of EFT transactions

The bank is liable for non-execution or deficient execution of payment transactions.[37] However, these rules are not absolute; a bank has the right not to execute a payment instruction employing an incorrect 'unique identifier'.[38] A 'unique identifier' is defined as 'a combination of letters, numbers or symbols specified to the customer by the bank and to apply by the customer in relation to a payment transaction in order to identify unambiguously the other user and/or

[36] *Ibid.*
[37] PSR 2009, regulations 74 and 76. Regulation 51 (3)(a) allows to the parties to agree not apply regulation 76 in case of business customer.
[38] *Ibid.,* regulation 74.

the customer's account for a payment transaction'.[39] The best examples of unique identifiers are a sort code of the bank and the customer's account number. Accordingly, the bank's obligation to execute correctly the payment instruction to the particular payee is dependent upon the employment of a correct unique identifier,[40] and in cases where the customer provides an incorrect unique identifier the bank is under no liability for non-execution or deficient execution of the payment instruction.[41] Thus, at first sight, the customer bears the losses of non-execution or deficient execution of the payment transaction when it is due to his negligence in providing an incorrect unique identifier. Furthermore, the customer bears the losses if the incorrect unique identifier provided by him leads to the wrong account being credited. However, a bank that employed an incorrect unique identifier bears liability, limited by their having made reasonable efforts to return the funds involved in the payment instruction.[42] Even so, a bank may charge the customer for its reasonable efforts to return the funds if so agreed in the banker-customer contract.[43]

The author's view is that, in practice, the parties' liability for using incorrect unique identifiers are: first, the bank bears no liability for any losses if it proves that it made all reasonable efforts, even if such efforts failed to recover the transaction's funds, so that here the customer bears the losses for non-execution or deficient execution of the payment instruction. Secondly, the customer will bear all losses if the bank proves that the customer acted with

[39] *Ibid.*, regulation 2(1).
[40] *Ibid.*, regulation 74(1).
[41] *Ibid.*, regulation 74(2).
[42] *Ibid.,* regulation 74(2)(a).
[43] *Ibid.,* regulation 74(2)(b).

gross negligence in providing an incorrect unique identifier.[44] Thirdly, the bank bears all losses if it executes a payment instruction employing an incorrect unique identifier knowing that the unique identifier is incorrect. The PSR 2009 does not include rules for dealing with the execution of payment instructions for a payee who does not exist or is unidentifiable. It seems that the PSR 2009 could be amended by establishing new provisions relating to execution of payment instructions for a non-existent or unidentifiable payee by ruling that the payee's bank must reject any such instruction.

Liability for non-execution or defective execution of the credit[45] and debit[46] transfer instructions is addressed as follows: first, liability of the payer's bank to the payer to execute the payment instruction correctly. The payer's bank is liable to debit the exact amount of the transaction and at the same time must be certain that the payee's bank credited the payee's account with the transaction funds by the end of the working day following the time of receipt of the payment order.[47] Thus, the payer's bank is liable for any losses, and must refund the payer the amount of the transaction if necessary, and also re-credit the payer's account.[48] However, the payer's bank has no liability to the payer when it is proved that the payee's bank received the transaction fund by the end of the working day following the time of receipt of the payment order. In debit transfer

[44] More details about customer's duty to exercise reasonable care and skill, see chapter three, section 3.4.1.
[45] PSR 2009, regulation 75. Regulation 51 (3)(a) gives the parties the right to agree not apply regulation 75 where the customer is a business.
[46] *Ibid.,* regulation 76. Regulation 51 (3)(a) gives the parties the right to agree to not apply regulation 76 where the customer is a business.
[47] *Ibid.*, regulation 70(1).
[48] *Ibid.,* regulation 70(6), 76(2), 76(5); Furthermore within regulation 77 the payer has the right to claim for any losses that he incurred as a result of non-execution or defective execution of the payment instruction. Regulation 51 (3)(a) gives to the parties the right to agree not apply regulation 77 where the customer is a business.

instructions, the payee's bank is liable to the payee for correct transmission of the payment instruction to the payer's bank within the time limits agreed between the payee and the payee's bank, enabling payment to be made within the agreed time.[49] The payee's bank must instantly re-transmit the payment instruction in question to the payer's bank.[50]

Secondly, the payee's bank will be liable to the payee for the transaction payment when the payer's bank has proved that the payee's bank received the transaction fund. Otherwise, thirdly, under the payer's request,[51] the payer's bank is obliged to investigate the whereabouts of the payment and notify the payer of the outcome.[52] If the outcome of the investigation is that the payment instruction was executed incorrectly, then the payer's bank will be liable to the payer and must re-credit the payer's account with the transaction fund without undue delay.[53] Furthermore, if the payer's bank fails to execute the required investigations to trace the whereabouts of the payment funds, an action for breach of a statutory requirement may be instigated and the payer's bank will be liable to the payer for any losses resulting from such a breach.[54] Nevertheless, the payer's bank obligation to investigate the whereabouts of the payment and notify the payer of the outcome can be excluded against business customers.[55] Fourthly, a bank is liable to its customer if it failed to follow due procedure. Such failure may also be evidence of negligence. Moreover, if a bank fails to comply with the Financial Conduct Authority (FCA) rules, a strict

[49] *Ibid.,* regulation 76(1).
[50] *Ibid.,* regulation 76(2).
[51] *Ibid.*, regulation 76(4).
[52] *Ibid.*, regulation 75(2).
[53] *Ibid.,* regulation 75(4).
[54] *Ibid.,* regulation 120(1).
[55] *Ibid.*, regulation 51(3)(a).

liability action can be brought against them under section 150 of the FSMA 2000. According to the FCA rule a bank 'must not seek to exclude or restrict, or rely on any exclusion or restriction of, any duty or liability it may have to a banking customer unless it is reasonable for it to do so and the duty of liability arises other than under the regulatory system'.[56]

This position is in contrast to the common law principles, wherein the law of agency is the main source of law applicable to the EFT parties' relationship. The agent owes to its principal a duty to exercise all the reasonable care and skill which a bank ought to exercise in execution of its customer's instructions. [57] In this context, the payer's instruction must be clear and unambiguous. Thus, if the payer's instruction to the bank is ambiguous, it is held that the payer's bank is under no liability for non-execution of the payer's instruction so long as it has taken all reasonable measures to execute the payment instruction.[58] On the subject of funds transfer instructions, the doctrine of strict compliance was rejected when Webster J in *Royal Products*[59] held that the doctrine of strict compliance cannot be applied to instructions of funds transfer. In this sense, as long as the payer's bank exercised all reasonable care and skill in executing the payment instruction it was not in breach of its mandate, and thus not liable for non-execution of its customer payment instruction. Therefore it is clear that the PSR 2009 changed common law principles.

[56] http://fshandbook.info/FS/html/FCA/BCOBS/1/1 28 November 2013.
[57] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194, at p. 198; *Lipkin Gorman (A Firm) Appellants and Cross-Respondents v Karpnale Ltd. Respondents and Cross-Appellants* [1990] 2 A.C. 548.
[58] *Midland Bank v Seymour* [1955] 2 Lloyds' Rep. 147, at p. 153, per Devlin J.; *European Asian Bank AG v Punjab & Sind Bank (No. 2)* [1983] 1 W.L.R. 642 at p. 656.
[59] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194, at p. 199; Further, see chapter three, section 3.4.2.1.

It seems that under the Regulation 2009 the main obligation of the payers' bank is executed the payment instruction given to it. The payer's bank may be liable even if it acts with all reasonable care and skill and was not negligent in the execution of the payment instruction. Furthermore, the payer's request to investigate and trace the whereabouts of the payment funds is not required to be handwritten. Thus, any action or saying from the customer could be interpreted as an implied request for investigation. In this regard, the customer could claim that he asked the bank for investigation in an implied request, such as asking for justification for the unavailability of his funds and then waiting for the bank to provide an explanation. The author's view is that subject to the potential liability of the payer's bank for non-execution or defective execution of the payer's orders, the strict liability is deemed to provide more protection to the payer and to make the payer's bank more circumspect in exercising its duty to execute the payment instruction.[60] However, the point of weakness with strict liability is that the customer will be in a powerful position and, as long as the bank bears the losses, the customer may not exercise reasonable care and skill in providing the bank with the EFT instruction. The PSR 2009 provisions fail to define the exact time of EFT finality. The author's view is that the payer's bank is liable for any losses as a result of non-execution or defective execution of the payment instruction even if it takes all reasonable steps with care and skill (strict liability). Thus, the payer's bank is required to refund and if necessary to re-credit the payer's account with the transaction funds. However, the payer's liability arises if the payer provided the bank with an incorrect unique identifier,[61] or wrongdoing is proved by the bank. In banking practice the bank will not be

[60] Ellinger, et al., *Modern Banking Law* (2011), p. 606.
[61] Lloyds TSB, *Personal Banking terms and conditions, October 2012*, *op.cit*, section C (8.1(b).

liable for any EFT instruction sent to the wrong payee if the payer gave the wrong details; nevertheless, the bank will exercise reasonable skills to recover the payment while imposing reasonable costs for such a service.[62] However, if the payer gave the correct details and the EFT payment was sent to the wrong payee it is the bank which is liable for the recovery of such losses.

It seems at first sight that the PSR 2009 cannot release the payer's banks from liability in the case of non-execution of the payment instruction. But this view can be rebutted. The payer's bank has no liability to the payer in the following cases: First, when the payer failed to inform the bank on becoming aware of any incorrectly executed payment instruction. Accordingly, the payer must, without delay and within a maximum of 13 months after the debit time, inform his bank of any incorrect instruction.[63] Secondly, when the execution of the payment instruction places the bank in breach of existing national law, such as anti-money laundering legislation. Thirdly, when there were abnormal and unforeseeable circumstances beyond the bank's control, with consequences which were unavoidable despite the bank's best efforts.[64] Finally, the bank has no liability to the payer for non-execution of the payments order if it is able to pass liability to the payee's bank or to a correspondent or intermediary bank, thus making its liability attributable.[65] The PSR 2009 potentially changes the common law rules by enabling the bank to pass its liability to the correspondent or intermediary bank.

[62] *Ibid.*
[63] PSR 2009, regulations 59(1) and 51(3)(b).
[64] *Ibid.,* regulation 79.
[65] *Ibid.,* regulation 78.

The author's view is that the PSR 2009 offers new rights to the customer with regard to the countermanding of payment instructions, implementation time and charges. Furthermore, it answers the question of when the payment is considered to be final by stipulating that the funds must be available to the payee by crediting the payee's account. However, the Regulations raise other problems without providing answers to them. For example: (1) the meaning of availability with regard to funds. (2) The issue of acceptance of the EFT instruction by the payee's bank and the extremely important question of when the inter-bank EFT payment is deemed final. (3) The meaning of defective execution, (4) funds discharged, (5) wrongful or non-exist payee. Consequently an attempt has been made to analyse the common law rules to find answers which will resolve these problems. The next section will investigate the principles of common law with regard to determining the finality of EFT transactions.

Table 4: Banks' Liability for non- execution payment instructions under Part 6 of the PSR 2009.

PSR 2009	**Regulation 75:** **Non-execution or defective execution of a credit transfer**	**Regulation 76:** **Non-execution or defective execution of a debit transfer**
Liability/ Obligation	Liability for non-execution or defective execution of the payment instructions	Liability for correct transmission of the payment order
Conditions	➢ Non-execution or defective execution ➢ Correct unique identifier provider by the payer: regulation 74(1)	➢ Not transmission of the payment instruction: regulation 76(1) ➢ Correct unique identifier provider by the payee: regulation 74(1)
Burden of proof	➢ Banks ➢ Accurate record, execution and entrance in the accounts of the transaction: regulation 75	➢ Banks ➢ Accurate record, execution and entrance in the accounts of the transaction: regulation 76

Consequences	➢ Refund of the transaction's funds to the payer due to the non-execution or defective execution: regulation 75(4) ➢ Restoration of the debited account of the former condition: regulation 75(4)	➢ Refund of the transaction's funds to the payer due to the non-execution or defective execution: regulation 76(5)(a) ➢ Restoration of the debited account of the former condition: regulation 76(5)(b)
Request	Not specified	Not specified
Limit exceptions	➢ Payment instructions executed according to the unique identifier deemed as correctly executed: regulation 74 ➢ In correct unique identifier provided by the customer: no liability of the bank: regulation 74(3) Force majeure, Community or national law, such as money laundering, no liability of the bank: regulation 79	➢ Payment instructions executed according to the unique identifier deemed as correctly executed: regulation 74 ➢ In correct unique identifier provided by the customer: no liability of the bank: regulation 74(3) Force majeure, Community or national law, such as money laundering, no liability of the bank: regulation 79

4.3 Revocation and completion of EFT payment under common law rules

4.3.1 Identifying the problem

There is a good case for the claim that an EFT instruction has been executed when payment has been made and the time available for revocation has elapsed.[66] In this regard 'completion of payment' can have more than one meaning. Firstly, it means the point where the payer loses the right to revoke the payment instruction. Secondly, it means the point at which the payee's bank has a liability to credit the payee's account. Consequently, it is important to find a method of defining the exact time at which the funds are credited. The problem is that there are differences between one EFT transaction and another and so it is not possible to define a single point at which the EFT becomes final. First of all, it is necessary to consider the legal nature of the money transfer process in question. For example, the time at which a funds transfer via BACS becomes irrevocable is different from the time that a bank giro credit is completed. In some cases, however, the time of completion of an EFT payment is determined in the banker-customer contract.[67] Secondly, the number of parties involved in the transaction and the function assumed by each party could affect the time of payment. There are intra-branch transactions in which the parties' bank accounts are held in the same branch of the same bank; and

[66] Arora, A., *Electronic Banking and the Law* (1988), p. 53; Cox, R. and Taylor, J., 'Funds Transfers', in Brindle, M. and Cox, R., (eds) *Law of Bank Payments* (2010), p.163.
[67] The Financial Markets and Insolvency (Settlement Finality) (Amendment) Regulations 2009 (SI 2009/1972).

there are inter-branch transactions in which the parties' bank accounts are held in different branches of the same bank. Then there are fund transfers involving accounts held in different banks (inter-bank). These inter-bank transactions can employ as many as five parties: the payer, the payer's bank, the correspondent or intermediary bank, the payee's bank, and finally the payee. For example, the payer's bank may request, by means of a telex from its correspondent, a credit to the payee's bank account. It is arguable that the payment is completed when the intermediary sends a message to the payee's bank. Nevertheless, the payee's bank may consider the payment incomplete until the transaction funds are actually credited to its account. Thus, the question of when the EFT payment is completed has different answers. In each case, a court would be dealing with a different point. It would be difficult indeed for the courts to establish a uniform principle defining the exact time at which the EFT is made.

In reaching a decision, the courts must take into account several points in time at which a payment may be considered as completed. These points could be: (1) when the payer's bank transmits the payer's instruction; (2) when the payee's bank, or its agent, receives the payment instruction;[68] (3) when the payee's bank acts on the payment instruction by crediting the payee's account on its computerised records;[69] (4) when the payee's account is actually credited with the transacted fund;[70] (5) when the payee is informed of the receipt of the

[68] *Mardorf Peach & Co Ltd v Attica Sea Carriers Corp of Liberia (The Laconia)* [1977] A.C. 850 at p. 880 and 889 per Lord Salmon and Lord Russell.
[69] *Joachimson v Swiss Bank Corporation* [1921] 3 K.B. 110 at p. 127 per Atkin L.J.
[70] *Eyles v Ellis* (1827) 130 E.R. 710.

transaction funds;[71] and (6) when the payee expressly or implicitly accepts receipt of the transaction fund.

4.3.2 Revocation of EFT payment

In the EFT contractual agreement the bank acts as agent to the customer.[72] Thus, the bank has to apply its customer mandate to transfer (credit transfer) or collect (debit transfer) a fund from one account to another.[73] However, the following points require clarification: First, the payer has the right to revoke the payment order as long as it has not been executed by the payer's bank. Second, the payer loses his right to revoke the payment order from the moment the bank acted on the payment instruction and transmitted the instruction to the payee's account. Thirdly, for a debit transfer order the payer loses his right to revoke the payment order from the moment the payer's bank acted on the payment instruction. Finally, the payee has the right to the money transferred after the payment order is executed. There is concern about revocation payment instruction with EFT. Cranston[74] presents general rules of revocation of payment instruction which apply in the non-existence of explicit agreement. He states:

> "In the absence of express contract, the authorities seem to establish the following propositions … Firstly, a customer who instructs its bank to hold funds to the disposal of a third party can countermand at least until the time when the funds have been transferred or credit given to the

[71] *Rekstin v Severo Sibirsko AO* [1933] 1 K.B. 47.
[72] Cranston, R., 'Law of International Funds Transfers In England' in Hadding, W., and Schneider, U.H., *Legal Issues in International Credit Transfers*, (1993), p. 232; Ellinger, et al., *op.cit.,* pp. 595-599; Hudson, P., and Mann, J. E., *Commercial Banking Law* (1978), p. 283.
[73] Cranston, *op.cit.,* p. 224 and p. 232; Arora, *op.cit.,* p. 50; Hudson and Mann, *op.cit.,* p. 283.
[74] Cranston, *op.cit*., p. 233.

> transferee. Secondly, a customer who instructs its bank to transfer funds to a third party cannot revoke from the moment the bank incurs a commitment to the third party. Thirdly ─ and this is the typical case ─ a customer who instructs its bank to pay another bank to the order of a third party cannot revoke once the payee bank has acted on the instructions. This may be a point prior to crediting the payee's account. In all cases, it is irrelevant, from the point of view of revocation, whether the third party has been informed."[75]

According to the Cranston rules, in the usual case where there is a paying bank and collecting bank in the EFT transaction, the customer's mandate is final and cannot be countermanded from the moment the collecting bank accepts the paying bank's payment instruction,[76] even though, to prevent any doubt as to the customer's right of revocation of the EFT instruction, the paying bank's agreement with the customer may consist of an express provision which prevents the customer from revoking the payment order after an exact point in the settlement procedures.[77] Otherwise, the customer must comply with the rules of the payment system used to make the funds transfer where those rules are applicable according to banking usage. Therefore, countermanding of payment orders will typically be a matter governed by explicit or implicit rules of the payment system involved in affecting the transfer.[78]

The EFT is completed only when the funds are actually credited in the payee's bank.[79] On the question of general rules, and with an absence of statutory rules, the common law has investigated 'payment finality' and seems to have recognised different, apparently incompatible positions.

---

[75] *Ibid.*
[76] Wood, P. R., *Comparative Financial Law* (1995), para, 25-18.
[77] *Report by the Review Committee on Banking Services: Law and Practice*, ("The Jack Report") (1989, London, HMSO, Cm 622), p. 105.
[78] For example, the Financial Markets and Insolvency (Settlement Finality) Regulations 1999.
[79] *Report by the Review Committee on Banking Services: Law and Practice*, *op.cit*., p. 103.

4.3.3 Completion of EFT payment

It has previously been explained that a credit transfer instruction is initiated by the payer ordering the bank to transfer funds to the payee's bank account, while a debit transfer instruction is initiated by the payee ordering his bank to withdraw the funds transaction from the payer's bank account. In a debit transfer, where the payee's bank withdraws funds from the payer's bank account, there is no doubt that the payee's bank acts as an agent for the payee.[80] Nevertheless, in credit transfers this position is uncertain. In this context, Cox and Taylor agree that the payee's bank collects the funds in a manner similar to that of any other settlement into a customer's account, thus the payee bank is acting as an agent to the payee.[81] This point is well demonstrated in *Mardorf Peach & Co Ltd v Attica Sea Carriers Corp of Liberia (The Laconia)* where the House of Lords held that a bank which has no actual or ostensible authority from the payee to accept a payment order cannot accept the transfer and credit the payee's account.[82] Although this case concerned the charter of a ship, it has general application to the law of agency. The creditor's bank received a telex message requesting it to credit the shipowner's account with the transaction funds under a charter party. The telex message was received at the creditor's bank after the date arranged in the charter party. The bank nevertheless began the process of crediting the ship-owner's account before it had received an order from the ship-owner to reject late payment. On receiving the order, however, it rejected the payment and returned the funds to

[80] Hapgood, M., et al., *Paget's Law of Banking* (2007), pp. 423-424.
[81] Cox and Taylor, Funds Transfers*, op.cit.,* p.165.
[82] *The Laconia* [1977] A.C. 850 at p. 866.

the payer's bank without carrying out the actual entry. The House of Lords held that the owners' bank had only limited authority to receive the payment and obtain instructions from the owners; it did not have authority to accept the late payment on behalf of the owners and had no authority to waive the owners' rights to withdraw the vessel.[83] Nevertheless the bank had taken delivery of the payment order and had begun to process it, these were held to be purely ministerial acts and, as such, provisional and reversible.[84]

The Laconia demonstrated that the finality of payment between the payer and the payee occurred only when the payee's bank has the payee's actual or ostensible authority to receive and accept the funds transfer on the payee's behalf. In this case, the ship-owners bank had no absolute authority; it had the authority to receive the funds transfer but not to accept the later payments on behalf of the owners.[85] King however has expressed disagreement that view, and explained that in credit transfer orders the contract between the payee's bank and the payee is not one of agency but one of banker and customer relationship.[86] King argues:[87]

> "it is inappropriate to say that the bank receives money paid by the customer into his own account as agent for the customer it is also inappropriate to say that the bank receives money paid by a third party for the account of the customer as agent for the customer."

---

[83] *The Laconia* [1977] A.C. 850 at p. 871.
[84] *Ibid.,* at p. 872.
[85] *Ibid.,* at pp. 871-872.
[86] King, R., 'The receiving bank's role in credit transfer transactions', (1982) 45 *the Modern Law Review* 369 at p. 369.
[87] *Ibid*., at p. 373.

Furthermore, King affirmed that in credit transfer orders the payee's bank is the agent or sub-agent of the payer.[88] According to this interpretation, in credit transfer orders the payee authorizes the bank to receive the payment not as payee's agent but according to normal procedure with its customer, the payee, as it would any other payment into a payee's account.[89] But King has been criticized by other legal authors[90] who have presented arguments to justify an assumption that the payee's bank should be regarded as an agent of the payee in the credit transfer order.[91] The reasoning is as follows: First, it is made clear that there are two contracts, the first contract between the payee's bank and the paying bank, and the second contract between the payee's bank and the payee. Therefore, when the payee's bank has received the funds transfers from the paying bank it is under duty of contract with the payee, so that the payee's bank ought to be constituted as an agent for the payee.[92] Secondly, the absence of an agency relationship between the payee's bank and the payee may lead to unauthorized fund transfers. If the payee's bank is not the payee's agent but the paying bank sends funds to the payee's bank without the authority of the payee then such a transfer would not discharge the payer's underlying indebtedness to the payee. Thirdly, one of the principles for the completion of payment between the payer and the payee is that the payee's bank should act as the payee's agent in receiving the funds before a credit is addressed to the payee's account. Fourthly, the absence of an agency relationship between the payee's bank and

[88] *Ibid.,* at p. 397.
[89] *Ibid.,* at p. 381.
[90] Goode, R. M., *Commercial Law* (2009), p. 579; Geva, B., *Bank Collections and Payment Transactions* (2001), p. 296; Cox and Taylor, Funds Transfers*, op.cit.,* p.163; Hapgood, et al., *op.cit.,* p. 424.
[91] Respectively, Geva, *Bank Collections and Payment Transactions*, *op.cit*., p. 296; Hapgood, et al., *op. cit*., p. 424.
[92] Geva, *Bank Collections and Payment Transactions, op.cit.,* pp. 296-297.

the payee results in an unsure distinction between different types of funds transfer so far as finality of payment is concerned.[93] The common law rules hold that in credit transfer payments the payee's bank acts as an agent of the payee.[94] The standing instruction in credit transfers is an order by the payer to the bank, as agent, to transfer a sum of funds from the payer's account to the payee's account. When the payee accepts payment by funds transfer it means that he accepts a right of action versus his own bank instead of his right of action versus the payer.[95] Such replacement of one debtor by another is similar to payment in cash and the payment between the payer and the payee is considered final.[96] However, there is too much ambiguity in identifying the exact time of replacement, when the payee's bank becomes the payee's debtor instead of the payer, for this to be the point where payment is final. In *The Brimnes,*[97] the charterers' bank in London, Hambros, had an account with the shipowners' bank in New York, MGT. The charterers by Telex instructed their bankers, Hambros, to credit the owners' account with a MGT, with the amount of the hire due. Hambros sent a Telex instruction to MGT to debit their account with the amount of the hire and credit it to the owners' account (to make an intra-branch funds transfer). The Court of Appeal held that the payment was complete when MGT decided to debit the account of Hambros, the payer's agent, and credit the account of the shipowners, the payee.[98] Accordingly, it is

[93] Hapgood, et al., *op.cit.,* p. 424.
[94] *Tenax Steamship Co v Brimnes(Owners of), The Brimnes* [1975] Q.B. 929; *The Laconia* [1976] Q.B. 835 at p. 847; [1977] A.C. 850; *Momm v Barclays Bank International Ltd* [1977] Q.B. 790; *Afovos Shipping Co SA v R Pagnan & Fratelli (The Afovos)* [1982] 1 W.L.R. 848 per Lloyd J.; *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194, at pp. 198-199 and pp. 201-203.
[95] Geva, B., 'Payment into a bank account', (1990) 5 *International Banking Law* 108 at p. 108.
[96] *Ibid.*
[97] *The Brimnes* [1973] 1 W.L.R. 386 at p. 400.
[98] *The Brimnes* [1975] Q.B. 929 at pp. 950-951 per Edmund Davies L.J., p. 964 per Megaw L.J. and p. 969 per Cairns L.J.

not necessary to inform the payee about the transfer, nevertheless, a decision to transfer need not have been executed, in whole or part, before the payment is considered final.

Even though, in the early stage of the same case, Brandon J. had that in "modern commercial practice"[99] this expression included:

> "any commercially recognised method of transferring funds the result of which is to give the transferee the unconditional right to the immediate use of the funds transferred."[100]

The concept of "unconditional" was broadly interpreted in *The Chikuma* where the House of Lords referred to unconditional to mean "unfettered and unrestricted", and that "the transferee's right to the use of the funds transferred is neither subject to the fulfilment of a condition precedent nor defeasible on failure to fulfil a condition subsequent.".[101]

It appears that EFT payment is considered final only when the payee is granted an absolute and unrestricted right versus the payee's bank to the direct use of the funds transferred. The question thus raised is: at what point does the payee obtain unfettered and unrestricted right versus the payee's bank?

[99] *The Brimnes* [1973] 1 W.L.R. 386 at p. 400 per Brandon J.
[100] *Ibid.*
[101] *Awilco of Oslo A/S v Fulvia SpA di Navigazione of Cagliari (The Chikuma)* [1981] 1 W.L.R 314 at p. 319(H) per Lord Bridge.

4.3.3.1 EFT finality in transactions between bank accounts held in the same branch of the same bank (intra-branch)

The completion of an EFT payment between the payer's account and the payee's account when both have an account in the same branch of the same bank occurs directly when the bank agrees to make the transfer,[102] assuming the payee's bank has an actual or ostensible (payee's) authority to accept payment on behalf of the payee,[103] regardless of whether the payee's account is credited with the money transferred and regardless of whether the payee has been informed of the transfer.[104] If the payee was informed of the transfer or if it was credited to the bank account this indicates to the court that the bank had decided to carry out the transfer. Nonetheless, there is nothing to prevent the payer and the payee from including in their contract the provision that payment is not considered final unless either of these circumstances has happened. *Eyles v Ellis*[105] was one of the initial cases dealing with intra-branch transfer. In this case the payer ordered his bank to transfer funds to the payee, whose account was in the same bank, in payment of rent. The bank executed the transfer and sent a letter to the payee informing of it. Meanwhile and before the payee received the letter, the bank became insolvent. The Court of Common Pleas held that the payment was final. The court's held Best C.J. judgment which was that payment occurred when the funds were actually transferred and

[102] This is not always the courts approach to the issue. See Cox and Taylor, Funds Transfers, *op.cit*., p. 167.
[103] The banker-customer relationship must be one of agency and not simply one of banker and customer, see Hapgood, et al., *op.cit*., p. 429; Cox and Taylor, Funds Transfers, *op.cit*., p. 167.
[104] *Ibid.*
[105] *Eyles v Ellis* (1827) 130 E.R. 710.

credited in the payee's account. Informing the payee was not directly related to the payment issue.[106]

Nonetheless, in *Rekstin v Severo Sibirsko AO*[107] the Court of Appeal did not refer to the *Eyles v Ellis* case. The absence of such a reference could be justified as it was not cited by counsel nor referred to in the judgments delivered in the Divisional Court or the Court of Appeal which could mean that the case did not become a judicial precedent. In *Rekstin,* the court held that the payment was considered final only when notice had been given to the payee informing him of the funds transfer. However, in this case the facts are unusual, the claimant, Rekstin, had a judgment against Severo, a Russian trading firm, the first defendant, who held an account at the bank which was the second defendant (the bank). To prohibit Rekstin levying execution upon the funds in that account, Severo instructed their bank to transfer the balance of their current account to another customer account of the same branch, and to close their account, this account being that of a Russian trade delegation with diplomatic immunity. On receipt of the instruction, the bank made the necessary inquiries and interest calculation to close Severo's account. Nevertheless, before a credit record could be placed in the trade delegation's account, the bank was served with *a garnishee* order nisi in regard of Rekstin's judgement versus Severo. The bank contended that, because of Severo's payment order and its own action, no debt existed as between them (the bank and Severo) at the time the *garnishee* order was served, therefore there was nothing on which the *garnishee* order could affect. At the time the *garnishee* order was served on the bank, Severo

[106] *Ibid.* at p. 711.
[107] *Rekstin v Severo Sibirsko AO* [1933] 1 K.B. 47.

did not owe any debt to the trade delegation, thus the trade delegation neither knew of, nor agreed to, the funds transfer which evidently made the bank under no liability to Severo.[108]

In *Rekstin* the Divisional Court[109] and Court of Appeal[110] it was held that Severo's payment order could be countermanded at the time when the *garnishee* order was served, and that service of that instruction functioned in law as a revocation. The courts[111] held that the payment should be considered complete when the payee has been informed that the funds had been posted to his account. Talbot J. held:

> "But in truth the bank never ceases to owe the money to the transferor until they have actually disposed of it according to his instructions; that is, paid it to the transferee and borrowed it from him. It is quite clear that this cannot be done by mere entries in the bank's books without communication with the transferee; if it could, there would be an interval during which the bank would owe the money to no one, not to the transferor, because the debt to him would on the hypothesis be cancelled, nor to the transferee, because there would be no privity between him and the bank."[112]

Lord Hanworth[113] held this view but nonetheless presented another reason to justify this opinion, based on *Gibson v Minet*,[114] where it was held that countermand of a payment order was acceptable as long as the payer's account was not debited and the payee's account was not credited with the sum transferred. Therefore Lord Hanworth M.R. held that Severo's payment order was countermanded at the same time as the bank was served with the *garnishee* order due to the fact that 'nothing amounting to a payment to the

[108] *Rekstin v Severo Sibirsko AO* [1933] 1 K.B. 47.
[109] Per Acton J. and Talbot J.
[110] Per Lord Hanworth M.R., Slesser L.J. and Romer L.J.
[111] The Divisional Court per Talbot J and Court of Appeal per Lord Hanworth M.R.
[112] *Rekstin v Severo Sibirsko AO* [1933] 1 K.B. 47 at p. 57.
[113] *Ibid.,* at p. 62.
[114] *Gibson v Minet* (1824) 130 E.R. 206.

delegation or an appropriation to their credit'.[115] According to Talbot J. the payment was to be considered final only if there was 'communication with the payee'. The author's view is that a typical communication method with the payee would be a letter from the payee's bank to the payee, or by any method agreed between them, such as telex or telephone message, informing the payee that the funds had been credited to his account. But what would happen, for example, if the payer ordered the bank to cancel notice of the payment to the payee by telex or telephone between the time the notice was posted and the time of receipt? Kerr J. in *Momm v Barclays Bank International Ltd* held that 'as a matter of law, the payer's bank would not have accepted revoking instructions from the payer after the process of crediting the payee's account had been set in motion pursuant to the payer's telex instructions'.[116] It can therefore be said that payment becomes final and cannot be countermanded at the time it is delivered to the payee's bank.[117] However, there is uncertainty at which point in time the payee's bank accepts transfer of the transaction's funds on the payee's behalf. [118] Kerr J. in *Momm v Barclays Bank International Ltd*[119] presented a response to the issue of the exact time at which payment has made to the payee, enabling the payee to use such funds in the same way as cash. In this case the claimant and the Herstatt Bank, a German bank, both had an account in a London branch of Barclays, the defendant. In accordance with the contract between the Herstatt and the claimant, on 25 June Herstatt ordered Barclays to pay £120,000 from their account to the claimant's account as part of a currency

[115] *Rekstin v Severo Sibirsko AO* [1933] 1 K.B. 47 at p. 64 per Lord Hanworth M.R.; Slesser L.J. and Romer L.J. followed this view, see p. 69 per Slesser L.J., and p. 71-72 per Romer L.J.
[116] *Momm v Barclays Bank International Ltd* [1977] Q.B. 790 at p. 802 per Kerr J.
[117] Ellinger, et.al., *op. cit*, p. 634.
[118] *Ibid.*
[119] *Momm v Barclays Bank International Ltd* [1977] Q.B. 790 at p. 802 per Kerr J.

exchange transaction. On 26 June 1974 the payment was duly made, and set in motion the appropriate computer processes to execute it in spite of the fact that Herstatt's account had insufficient funds. Later on the same day it became known by Barclays that Herstatt suspended payment. However no action was taken by Barclays and therefore the transfer from Herstatt to the claimant was completed by the bank's central computer at the end of the day. Although the final transfer was shown on the bank's central computer Barclays did not reverse certain transactions until the following day. When the claimant later discovered what had occurred it claimed that the transfer had been irrevocable and that Herstatt Bank had wrongfully debited its account with £120,000.[120] The judgment was for the claimant. Kerr J. held that the payment between the Herstatt and the claimant became final at the moment Barclays accepted Herstatt's orders to credit the claimant's account and the computer processes were set in motion.[121] In *Momm*, the court held that the finality of payment between the payer and the payee was not conditional upon the payee being informed.[122] Kerr J. held:

> "although the defendants did on occasion reverse certain transactions when the final balances had been produced by the central computer the day following the transactions, their transfer … was not a conditional transfer; that, accordingly, the transaction was completed on June 26 when the defendants accepted H's instructions to credit the plaintiffs' account and the computer processes were set in motion; and that, therefore, after the close of working hours on June 26, the defendants were not entitled to debit that sum from the plaintiffs' account even though the original transfer had not been notified to the plaintiffs."[123]

[120] *Ibid.,* at p. 792.
[121] *Ibid.,* at p. 791.
[122] *Ibid.,* at p. 791.
[123] *Ibid,* at p. 791.

Kerr J. distinguished *Rekstin v Severo Sibirsko AO* as a case where decided on its special facts.[124] Kerr J. emphasised that what was significant in *Rekstin* was that the payee had no knowledge of the proposed transfer, that there was no underlying transaction between the payer, Severo, and the payee, the trade delegation, and that the payee's account had never been credited with the funds that were supposedly transferred to it.[125] Indeed, in *Rekstin* the bank had no authority from the payee to receive the funds on its behalf. The bank had no actual authority to receive the funds because the payee knew nothing of it, nor could they have expected that it would be made. Moreover, there was no ostensible authority to receive the funds because the payer was aware that there was no reason for the transfer to be passed, apart from the protection of its own interest. Thus the payment to the payee, (the trade delegation), had not been made because it had not received notice of the payment. By contrast, in *Momm* there was a currency exchange contract between Herstatt and the claimant by which the payment should have been transferred into the claimant's account at Barclays. Thus, the bank obviously had the claimant's authority to receive the funds on the claimant's behalf.

It is suggested that the most significant point of Kerr J.'s decision is that the time of payment finality was when the payee's bank agreed to credit the payee's account.[126] Moreover it is suggested that Kerr J.'s reference to the fact that the bank had begun the computer operation for affecting the transfer is additional evidence of the bank accepting to credit the payee's account. Although, Cox and Taylor argued that evidence of the bank accepting to credit the payee's

[124] *Ibid.,* p. 800.
[125] *Ibid.,* at p. 801.
[126] *Libyan Arab Foreign Bank v Bankers Trust Co.* [1989] Q.B. 728 at p. 750 per Staughton J.

account could be available from different resources, for example, the bank's own authorization slips or other internal memoranda.[127] Nonetheless, the bank must accept the transference of an absolute credit right to the payee's account in order for the payment to be considered final. Consequently, the granting of conditional or provisional credit would argue for subsequent reversal.[128] In *Momm* such a point was not considered problematical because the transfer of funds took place in the same branch of the same bank. In other cases, nonetheless, it is clear that there could be a problem, since the bank may be uncertain of being put in funds and so agrees to make only a provisional credit to the payee's account pending the receipt of the transactions' funds. The question thus arises: must the payee's account be credited to indicate that the payment is completed?

In *Momm* the court considered the finality of payment to be at the moment the bank agreed to credit the payee's account, the actual credit being no more than a report of the earlier payment. Although, this view conflicts with *Eyles v Ellis*, it is consistent with the approach taken in *The Brimnes* by Brandon J. and confirmed by the Court of Appeal,[129] which held that the payment was complete when the payer's bank decided to debit the account of the payer's agent, payer's account, and credit the account of the payee.[130] Within such case, it appears that informing the payee is not important, and also that a decision to transfer need not have been executed, in whole or in part, before the payment

[127] Cox and Taylor, Funds Transfers, *op.cit*., p. 170.
[128] For example, see *Sutherland v Royal Bank of Scotland Plc* [1997] S.L.T. 329.
[129] *The Brimnes* [1975] Q.B. 929, see above pp. 187-188.
[130] *Ibid.,* at pp. 950-951 per Edmund Davies L.J., p. 964 per Megaw L.J. and p. 969 per Cairns L.J.

is considered final.[131] Geva[132] has argued that designating the posting of a credit to the payee's account as the time of payment creates two uncertainties. These are: 'First, the credit posted to the account may be provisional or conditional upon arrival of funds, the posting of a provisional credit to a payee's account cannot be viewed as conferring upon him an 'unfettered and unrestricted' right, as required. Second, the exact time of finality or irreversibility in the internal system of posting a credit to an account may not be definitely established.'[133]

Nevertheless, considering the time of crediting the payee's account as the time of completion of payment raises difficulty as same as which may arise in practice,[134] since a court has to determine the exact moment when the bank made a decision to debit the debtor's account and credit the creditor's account. Cox and Taylor agree that in practice, it is very difficult to determine the exact moment of the decision to make the transfer.[135] In *Momm* Kerr J. introduced rules which could be useful to apply when it is impossible to define the exact time of the bank's decision to make the transfer. Kerr J. held that:

> "a payment has been made if the payee's account is credited with the payment at the close of business on the value date, at any rate if it was credited intentionally and in good faith and not by error or fraud."[136]

According to this view, it seems that, while it is impossible to point to an exact moment when a 'decision' has been made by the bank to make a transfer, it is to be expected that the transfer will have been made at the end of the business

[131] Cox and Taylor, Funds Transfers, *op.cit*., p. 171.
[132] Geva, *Bank Collections and Payment Transactions, op.cit.,* p. 276.
[133] *Ibid.*
[134] Cox and Taylor, Funds Transfers, *op.cit*., p. 171.
[135] *Ibid.*
[136] *Momm v Barclays Bank International Ltd* [1977] Q.B. 790 at p. 799.

day on which the transfer note is processed.[137] In *Momm* the court found it unnecessary to define the exact moment in the day at which the payment was made. The important issue in the case was to determine whether the payment was final on 26 June before it was reversed on the following day. By contrast, in *Rekstin* the exact time of payment was not required because the court concentrated on the moment the actual credit was made to the payee's account and this focus possibly provided the court with positive evidence that the payment was final. Mann[138] considers it unacceptable for the finality of payment to be the moment when the bank accepts to debit the payer's account and to credit the payee's account without actual credit. His view is that the payment is to be considered final when the payee has the right to use the funds as an equivalent to cash. Mann states:

> "it is submitted that such result [the payment is final when the bank agreed to debit the debtor's account and credit the creditor's account without actual credit to the payee's account][139] are unacceptable, for so long as the recipient's account has not been credited he is unable to dispose of the money. The possibility of immediate and unconditional use of the money should be the test of effective payment. Nothing short of a credit entry achieves this."[140]

Hapgood, et al,[141] Cox and Taylor[142] agree against Mann's approach for the following reasons: first, Mann's approach does not take into account that a chose in action can arise in the payee's favour without actual credit to his account. If it were otherwise, the bank could allege that it was not indebted to the payee whenever, as a result of the bank's computer mistake, it fails to credit

[137] Cox and Taylor, Funds Transfers, *op.cit*., p. 172; Geva, *Bank Collections and Payment Transactions, op.cit.,* p. 278 and p. 280.
[138] Mann, F. A., *The Legal Aspect of Money* (1992), p. 85.
[139] The words in square brackets added.
[140] Mann, *op.cit.,* p. 85.
[141] Hapgood, et al., *op.cit*., pp. 429.430.
[142] Cox and Taylor, Funds Transfers, *op.cit*., p. 172.

a fund to the payee's account. Secondly, Talbot J. in *Rekstin* considered that the 'mere closing of an account does not discharge or cancel the bank's debt to the customer; the bank owed the customer the funds until it paid', such fact being considered as evidence for the underlying debt. Ultimately, considering the payment is made between the payee and the payer only when the payee's account is actually credited, it would cause the payer to owe the payee until the payee's bank's procedure is completed, that is, to owe the payee during the period between the time when the payee's bank decided to make the payment and the time of the actual crediting of the payee's account.[143] In conclusion, intra-branch fund transfers are considered final when the bank agrees to make the payment, regardless of whether the funds have been credited to the payee's account. However, any agreement between the payer and the payee for allowing a particular time for the completion of the payment must be taken into account.

4.3.3.2 EFT Finality in transactions between bank accounts held in different branches of the same bank (inter-branch)

Momm defined the finality of payment in cases involving intra-branch fund transfers. However, there is no obstacle to applying *Momm*'s rules in cases of inter-branch fund transfers.[144] Thus, according to *Momm'*s rules, payment is final when the bank agrees to credit the payee's account absolutely, supposing that the bank has the payee's actual or ostensible authority to accept the funds

[143] *Ibid.*, at p. 173.
[144] *Ibid.*

transfer on the payee's behalf. Inter-branch fund transfers, however, are subject to particular problems, for example, when the payer's bank has agreed to make an inter-branch transfer on behalf of the payer but the payee has ordered his bank to refuse all transfers from that payer. The answer could be simply that, unless otherwise agreed, the customer has the right to request refunds only at the branch where his account is located.[145] Therefore, the most significant branch in determining the finality of an inter-branch EFT is the payee's branch where the latter's account is held as the payee and the payees' bank relationship is concerned.[146] On this ground, the payment between accounts held in different branches of the same bank is considered final when the payee's branch agrees to make the payment and to credit the payee's account.[147]

4.3.3.3 EFT Finality in transactions between bank accounts held in a different banks (inter-bank)

EFT transactions may involve accounts held at different banks. The finality of payment between the payer and the payee takes place when the payee's bank accepts the payment instruction from the payer's bank and agrees to make unconditional credit to the payee's account with the transaction fund, assuming that the payee's bank has the payee's actual or ostensible authority to accept

[145] *Joachimson v Swiss Bank Corporation* [1921] 3 K.B. 110 at p. 127 per Atkin L.J.
[146] Cox and Taylor, Funds Transfers, *op.cit*., p. 173.
[147] *Libyan Arab Foreign Bank v Manufacturers Hanover Trust Co (No.2)* [1989] 1Lloyd's Rep. 608.

payment on the payee's behalf.[148] Regardless of whether the payee's bank has actually credited the payee's account and regardless of whether it has informed the payee of the transfer.[149] Nevertheless, the actual crediting of the payee's account or notice to the payee of the transfer will be significant evidence for the claim that the payee's bank has agreed to make the payment on the payee's behalf.[150] However, any agreement between the payer and the payee must be taken into consideration. Therefore if the agreement establishes that the payment is considered final only when the payee's bank has actually credited the payee's account or when the payee has been informed of the transfer then the payment is considered final only when such conditions have been executed. [151] Consequently, as soon as the payee's bank has accepted unconditionally a payment to credit the payee's account, it confirms that the payee is one of its creditors and such an agreement makes it a substitute for the payer as the payee's debtor. Payment between the payer and the payee is then constituted as final.[152] Receive of funds on the part of the payee's bank to make the payment and to credit the account with the funds transfer is insufficient to consider that the payment has been made.[153] The payee's bank must accept these funds for the payee's account which is vital. There are many significant legal circumstances which permit the bank to decline the transfer of

[148] *The Laconia* [1977] A.C. 850; *The Chikuma,* [1981] 1 W.L.R 314.
[149] *The Laconia* [1977] A.C. 850 at p. 880 per Lord Salmon and p. 889 per Lord Russell.
[150] *Empresa Cubana de Fletes v Lagonisi Shipping Co Ltd (The Georgios C)* [1971] 1 Q.B. 488 at p. 503, the court held that the payment slip which was sent from the payer's bank to the payee's bank as 'a banker's payment slip'. Therefore, according to Lord Denning M.R. such slip is equivalent to cash.
[151] Cox and Taylor, Funds Transfers, *op.cit*., p. 175.
[152] *The Laconia* [1976] Q.B. 835 at p. 847, Lord Denning held that: "If the paying bank had sent actual currency, the payment will be made when it was handed over the counter to the receiving bank, and accepted without objection. So also with the 'payment order'. It is equivalent to cash paid over to the receiving bank. If accepted without objection, it is the equivalent of its customer himself accepting cash without objection." .
[153] Cox and Taylor, Funds Transfers, *op.cit*., p. 175.

funds to the payee's account. For example, the bank may have no authority from the payee to accept the payment order, or the bank cannot accept the payment order to credit the payee's account without breaking some existent law, the existing law may prohibit credits being passed to the account of certain foreign nationals.[154] Consequently, until the payee's bank has agreed to make a funds transfer to the payee's account it acts as agent for the payer. However, funds transferred from the payer's bank account to the payee's bank constitute final payment between the payer and the payee only if it is credited in the payee's bank, which has the payee's actual or ostensible authority to receive and accept the payment, and the payee's bank was informed of the details of where the payee's funds were to be credited.[155]

The next issue is whether acceptance of the funds transfer by the payee's bank is designated as the point of finality of payment. The answer is that once the payee's bank agrees to credit the payee's account unconditionally, it accepts a credit risk so that it becomes indebted to the payee and payment between payer and payee is final.[156] As explained above, payment as between payer and payee will be final only when the funds are credited to in the payee's bank which has the payee's actual or ostensible authority to receive and accept the payment on the payee's behalf. In some cases, the payee may give the payer actual notice by informing him not to pass further payments. Therefore, any further payment from the payer would be outside the terms of the underlying agreement between them. In such case the payee's bank itself has no actual or

[154] Goode, *op.cit.*, p. 508.
[155] *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194; Cox and Taylor, Funds Transfers, *op.cit.,* p. 175.
[156] Cox and Taylor, Funds Transfers, *op.cit*., p. 175.

ostensible authority to receive and accept this payment on the payee's behalf. In this respect the payee has the right to exert his authority to make the bank accept that payment. This extension of authority has to be imposed before the payee's bank rejects the payment. In *the Laconia,* Lord Salmon held that: 'the ship-owners could have been considered to have accepted the payment if their bank had kept it for an unreasonable time. EFT finality occurred when the payee's bank accepted the payment on behalf of the payee and credited the funds to his account.'[157] Ultimately, in the inter-bank transfer the legal nature of transfer is conditional, and thus, the EFT is completed only when the funds are actually credited to the payee's account and can be used by the payee as equivalent to cash.[158] Thus, the payee must has 'unfettered and unrestricted' rights to use the transaction funds for the payment to be considered final. Geva confirms that, so far as the execution of rules is concerned, English courts have failed to provide a fully consistent scheme for determining the 'finality of payment'.[159] therefore, it is the delay prior to the point at which funds are credited to the payee's account which led courts to find an earlier point of finality, for example, the receipt of a payment instruction by the payee's bank, a concept that later fell out of favour; or the point at which the payee's bank decides to credit the payee's account.[160]

Given the above exposition, it seems that banking practice has developed over the years and such development leads to the requirement of rules subject to the payer's right to revoke payment or to demand a reversal of entries. The author's

[157] *The Laconia* [1977] A.C. 850 at p. 880.
[158] *The Chikuma* [1981] 1 W.L.R 314.
[159] Geva, B., 'Payment finality and discharge in funds transfers', (2008) 83 *Chicago-Kent Law Review* 633 at p. 645.
[160] *Ibid.*

view is that the absence of any particular rules to apply to EFT finality leaves the courts with no option except to draw an analogy with the finality of the clearing cycle of cheques, which is determined exclusively by banking practice. The analogy, however, must be taken from cases which determine the time at which payment by cash is completed between the payer and payee.

The author's view is that, first of all, an EFT between banks, or between a bank and its customer, is to be considered final when the transaction fund is irrevocably available to, and accepted by, the payee's bank.

However, in this context, it is worth noting the banker's right to "set off" or "combine" accounts. Where a customer keeps more than one account with his bank, the bank has a general right to set off a credit balance on one account against a debit balance on another account. The existence of the right of set off does not depend on any express term in the banker-customer contract.[161] However, it may be excluded by an express term in the contract prohibiting the bank from combining its customer's accounts. In the absence of any exclusion, the bank can transfer money from an account that is in credit in order to make payments due on another account.[162] Where a customer has an overdrawn account, the bank can also use the right of set off to apply any funds received on behalf of the customer in reducing the overdrawn balance. In the context of EFT "set off" is important because it gives the payee's bank some control over what happens to funds received on the payee's behalf. So, if a payee has an overdrawn current account and a savings account with a credit balance and the bank then receives funds on the payee's behalf, the bank can use the right of

[161] *Garnett v M'Kewan* (1872) LR 8 Ex., at pp. 10, 13, and 14; *Cinema Plus Ltd v ANZ Banking Group Ltd* (2000) 35 ACSR 1.
[162] Further details, see Ellinger, et al., *op.cit.,* pp. 248-266.

"set off" to apply the funds in reduction of the overdraft (regardless of whether the payee has directed the funds to be applied to the savings account). Financial Ombudsman Services clarifies that there must be certain conditions before a bank can exercise its right of "set off". These conditions are: first, the account from which the bank transfers funds must be held by the customer who owes the bank money; secondly, the debt must be due and payable.[163]

In this regard, it is important to explain that "netting"[164] and "set off" are really significant issues in the context of bankruptcy/insolvency. Suppose A owes B £1 million and B owes A £1 million. In the absence of any "netting" or "set off", these would be treated as separate liabilities. This is important and can have dramatic consequences. If B were to become bankrupt, then A would still be liable to pay £1 million to B's trustee in bankruptcy, for example, the official responsible for administering B's affairs following his bankruptcy, but A would have to compete with all of B's other creditors to get any of the £1 million owed to him by B. If B's total assets amount to £5 million, but his total debts amount to £100 million, then each creditor is going to receive 5% of what they are owed. Therefore, A will end up having to pay his debt to B of £1 million in full, but receiving back only with £50,000 of the total debt of £1 million from B's bankruptcy. So, without any netting or set off, A would effectively lose £950,000. In contrast, if A can set off his debt to B against the debt owed to him by B, then A does not have to pay anything at all to B's trustee in

[163] Financial Ombudsman Services, issue 40, http://www.financial-ombudsman.org.uk/publications/ombudsman-news/40/40_setoff.htm 29 November 2013.
[164] See chapter one, section 1.2.

bankruptcy. In this example, the £1 million debts will effectively cancel each other out.

Finally, “set off”, which applies between banks and their customers, may therefore be important for a bank in cases where its customers become bankrupt. This is quite different from the concept of “netting”, which is concerned with the settlement of reciprocal payment obligations between banks,[165] is likely to be even more important, because of the amounts involved, for a bank in cases where another bank becomes insolvent.

Secondly, the EFT between the payer and the payee is to be considered final when payment acts as an unconditional order of the payee. It appears that there is a need to regulate the EFT completion principles by means of a statutory instrument, or at least to find a general principle applicable to all the cases in question.[166]

[165] Further about “netting” see chapter one, section 1.2.
[166] See chapter seven, section 7.3 for the author’s proposal model of EFT finality rules.

Table 5: Comparison points between the PSR 2009 and Common law in the EFT finality.

Attributes	PSR 2009 provisions	Common law rules
Revocation	The payer has the right to revoke as long as the payee's account is not credited	The payer has the right to revoke as long as the payer's bank did not execute the payment instruction
Accepting the payment instruction by the payee's bank	Not applicable	The payee's bank must accept the payment instruction
Finality of payment	➢ Credited the payee's bank account; or ➢ Credited the payee's account and there is no place to make any condition or provision on the receiver funds	➢ Debited the payer's account; or ➢ Accept the payee's bank the transaction funds
Value available	Equal to cash	Not actually is available to the payee similar to cash
Liability of the payer's bank	Strict liability	Exercise all reasonable care and skill

4.4 The legal nature of payment devices

If the payer makes a payment to the payee using one of the EFT devices, for example, a debit card or a credit card, and all goes well, the outcome will be a debit of the payer's bank account and a credit of the payee's bank account. All significant stages of the transaction between payer and payee will have been completed. But assume that between the time the payment instruction was issued and the time that it would have been completed, one of the banks participating in the EFT operation became insolvent. The problem then is to decide whether the payment instruction has continued to the point where the payer's responsibility to the payee has been settled, or whether the payee can still proceed against the payer according to the underlying agreement regarding responsibility. The legal nature of the funds transfer and the legal nature of payment methods serve to determine which party bears the risk in cases of bank insolvency. Earlier, the legal nature of the funds transfer was explained. In the next sections the legal nature of the payment devices will be examined in order to determine which party bears the risk of non-payment in the context of EFT transactions.

4.4.1. The conditional payment

Generally, payment by cards is one of the EFT transactions which are described as a debit transfer. As a result of a debit transfer order the payee's bank account is credited and the payer's bank account is debited. In this

settlement operation the payee's bank is acting as an agent for the payee.[167] It is difficult to determine whether an EFTPOS payment (debit card payment) is a debit transfer order or a credit transfer order. The point is best clarified by answering the following questions, viz: did the payer order his bank to debit his account and transfer the fund to the payee's bank account? Or did the payee order his bank to credit his account by collecting the funds from the payer's bank and the payer's bank debiting payer's account? The answer could be either credit transfer or debit transfer. In practice, payer and payee issue a communication that goes to a data processing unit which is acting on behalf of both the payer's bank and the payee's bank.[168] That data processing unit contacts the payer's bank and establishes whether the card is authorized and whether the payer, the cardholder, has sufficient funds to pay for the transaction. The normal outcome of the data processing is that the cardholder's account will be debited and the payee's account credited. Normally there is an underlying obligation between the cardholder and the payee. Thus, the issue is, after the payment transaction order takes place how has the underlying obligation has been affected, assuming that the payment order was rightly executed by the payer. What if, however, the transaction's funds did not credit the payee's account so that the payment is not made? Does the payee have the right to claim payment due to the underlying obligation? The main right of the contract between the payer and the payee is the supply of goods and services

[167] Particularly, see *The Laconia* [1976] Q.B. 835 at p. 847, per Lord Denning; *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 at pp. 198-199 and pp. 201-203, per Webster J.
[168] Rogers, J. S., 'Unification of payments law and the problem of insolvency risk in payment systems', (2008) 83 *Chicago Kent Law Review* 689 at p.709.

to the payer, and the main obligation is payment at the same time.[169] If the obligation is not fulfilled the answer could be that the payee has the right to claim the payment due to the underlying obligation. Nevertheless, to answer this question it is necessary to analyse the legal nature of payment by debit card.

There is a legal view which considers payment by debit cards as an absolute payment.[170] Ellinger, et al.[171] Smith and Robertson[172] strongly support such a view and they agree that payment by debit cards is dissimilar to payment by cheque. There is dissimilarity in legal nature, however, when the debit card holder does not have credit.[173] According to Smith and Robertson's view it can reasonably be argued that the payment order took place once the payer and the payee issued the payment order and the payer's bank debited the payer's account. They also argue that any agreement between the cardholder, the payer, and the payer's bank has to be taken into account, so that if the agreement establishes that the payer's bank guarantees payment by debit cards by issuing an authorized overdraft facility the bank will be liable to make the payment. Consequently, the payer and the payer's bank may consider payment by debit card absolute, as a result of which the payee has no right to demand the cardholder to pay again under any circumstances,[174] such as in the event of the insolvency of the payer's bank. Ellinger[175] et al. state that under debit cards schemes the bank and not the holder is liable to the payee for

[169] Blackstone, M. R., *Blackstone's Sale and Supply of Goods and Services* (2001), p. 251; Sale of Goods Act 1979, section 27.
[170] Guest, A. G., *Benjamin's Sale of Goods* (2006), para. 9-033; Ellinger, et al., *op.cit.,* p. 660; Smith and Robertson, *op. cit*., p. 248.
[171] Ellinger, et al., *op.cit.,* p. 660.
[172] Smith and Robertson, *op.cit*., p. 247.
[173] *Ibid.*
[174] *Ibid*.; Ellinger, et al., *op.cit*., p. x\660; Rogers, *op.cit*., p. 710.
[175] Ellinger, et al., *op.cit.,* p. 660.

payment. He stated: 'in case of the risk of bank insolvency the payee has no right to claim the card-holder (payer) to pay again.' But such an argument depends on the transaction having been affected'.

It should be noted here that the legal nature of payment by debit card is conditional, although it could have an absolute nature: in cases where there are insufficient funds in the customer's account and there is no authorized overdraft agreement. The bank is under the duty to make payment with regard to the customer's mandate[176] only if the customer has enough money in his account or has obtained an overdraft facility from the bank by prior agreement. Therefore, if there is insufficient credit or there is no overdraft facility the bank is not obliged to pass payment and has the right to reject the payment mandate on the basis of inadequate funds.[177] In this regard, it has been submitted as a general principle of law that a payment by debit card is conditional. Therefore, if the bank failed to pay it by reason of insolvency the drawer who is under obligation has to pay and the risk will be on him.[178]

Nonetheless, the conditional nature of payment by debit card applies if there is no overdraft facility and the funds are withdrawn from the payer's current account.[179] Therefore, if there is an overdraft facility, payment by debit card is considered absolute and the bank will be liable to make payment to the payee.[180] Overdraft is one of the bank's facilities to customers who open current accounts and it authorizes the customer to withdraw even when his balance is

[176] *Fleming v Bank of New Zealand* [1900] A.C. 577.
[177] Arora, *Electronic Banking and the Law*, *op.cit*., p. 46.
[178] *Re Charge Card Services Ltd* [1989] Ch. 497.
[179] Smith, G. J. H., et al., *Internet Law and Regulation* (2007), p. 885.
[180] *Re Charge Card Services Ltd* [1989] Ch. 497.

in debit.[181] The customer's balance will be owed to the banker. The banks grant the customer an overdraft according to an agreement between the bank and the customer, which is a planned overdraft; however, the customer may have such a facility even if there is no agreement, which is an unplanned overdraft.[182] The planned overdraft puts the bank under an obligation to make the payment on behalf of the payer,[183] whereas if the overdraft is unplanned the bank can refuse to make the payment.[184] In practice, even if there is no agreement allowing customers to obtain an overdraft they may, with the bank's approval, be provided with an unauthorized overdraft to cover the payment.[185] The bank is free to choose whether or not to allow such a facility. Nevertheless, the customer must be aware of the interest charges and know that payment will have to be made to the bank if the overdraft occurred without authorization.[186] The unplanned overdraft is considered as an implied request from the customer to the bank to grant an overdraft facility.[187] If the overdraft facility was arranged between the parties then the bank must make the payment and the customer is indebted to the bank.

[181] For example, Lloyds TSB, *Personal Banking terms and conditions 2012*, section C(10) http://www.lloydstsb.com/media/lloydstsb2004/pdfs/personal_banking_terms_and_conditions.pdf; HSBC, *General Terms and Conditions, Current Account Terms and Conditions 2012*, section 3 http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf; Barclays, *Customer Agreement 2012*, section 5 http://www.barclays.co.uk/ImportantInformation/TermsandConditions/P1242575350746 9 April 2013.
[182] *Ibid.; Office of Fair Trading v Abbey National* [2008] C.T.L.C. 1.
[183] *Barclays Bank Ltd v WJ Simms Son and Cooke (Southern) Ltd* [1980] Q.B. 677 at p. 699 per Goff J.
[184] Barclays *Customer Agreement*, section 4(4.5) http://www.barclays.co.uk/ImportantInformation/TermsandConditions/P1242575350746 9 April 2013.
[185] *Office of Fair Trading v Abbey National* [2010] 1 A.C. 696.
[186] *Ibid.*, at p.755.
[187] *Lloyds Bank Plc v Independent Insurance Co Ltd* [2000] 1 Q.B. 110 at p. 118.

Where there is an unauthorized overdraft facility the bank may not immediately grant such a facility but may undertake various processes in order to determine whether or not to allow such a facility. It is well known that when a customer requests overdraft facilities, whether implicitly or explicitly, the bank is free to grant or disallow such a facility without being in breach of banker-customer contractual duties.[188] However, to protect the customer the bank must prove that it is acting in accordance with banking practice and the banking code.[189] Arora[190] agrees that the bank has discretion to pay in accordance with the customer mandate an order that will enable the customer to obtain an overdraft facility. But, he argues that the bank will be in breach of the contractual relationship with the customer if, in not granting an overdraft facility, it acted arbitrarily, capriciously or in bad faith.[191] In this sense, the bank has the right to refuse to grant any overdraft on reasonable grounds. Furthermore, in practice the banks protect themselves by establishing that they are absolutely free to allow or disallow unauthorized overdrafts, while being under no obligation to present justifications for their decision. Therefore, the legal nature of payment by debit card is conditional.[192] In this regard, if the payee's account was not

[188] *Office of Fair Trading v Abbey National* [2008] C.T.L.C. 1 at p. 81 per Andrew Smith J.; Lloyds TSB, *Personal Banking terms and conditions*, section C(10) http://www.lloydstsb.com/media/lloydstsb2004/pdfs/personal_banking_terms_and_conditions.pdf; HSBC, *General Terms and Conditions, Current Account Terms and Conditions,* section 3, http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf; Barclays *Customer Agreement*, section 5 http://www.barclays.co.uk/ImportantInformation/TermsandConditions/P1242575350746 9 April 2013.

[189] *Office of Fair Trading v Abbey National* [2008] C.T.L.C. 1.

[190] Arora, A., 'Unfair contract terms and unauthorised bank charges: a banking lawyer's perspective', (2012) 1 *Journal of Business Law* 44 at p. 50.

[191] *Ibid.*

[192] Goode has support this view and he considers payment by debit card only a modern electronic payment, similar to cheque, Goode, R. M., *Consumer Credit Law and Practice* (loose-leaf), para,1A[3.50], 1C[25.83], 1C[25.84]; Guest, A. G., and Lloyd, M., *Encyclopaedia of Consumer Credit Law* (1974), para,1A[3.50], 1C[25.83], 1C[25.84].

credited with the transaction funds he can request the payer/ cardholder to pay again. It is reasonable and fair to grant customers overdrafts to make payments for their transactions. In this respect, the debit card payment is absolute.

4.4.2 The absolute payment

It is the general rule that, when the payer pays with a plastic card, the payer's account is responsible, directly or indirectly, for payment in the transaction. The legal nature of payment by credit card in English law constitutes unconditional payment because of the contractual schemes explained below (figure 8, page 229). Thus, it is considered a convenient method of payment from both the payee's and the payer's perspective.[193] The legal nature of credit cards has been established in English courts through the decision in *Re Charge Card Services*[194] which held that the legal nature of payment by credit cards is an absolute payment.

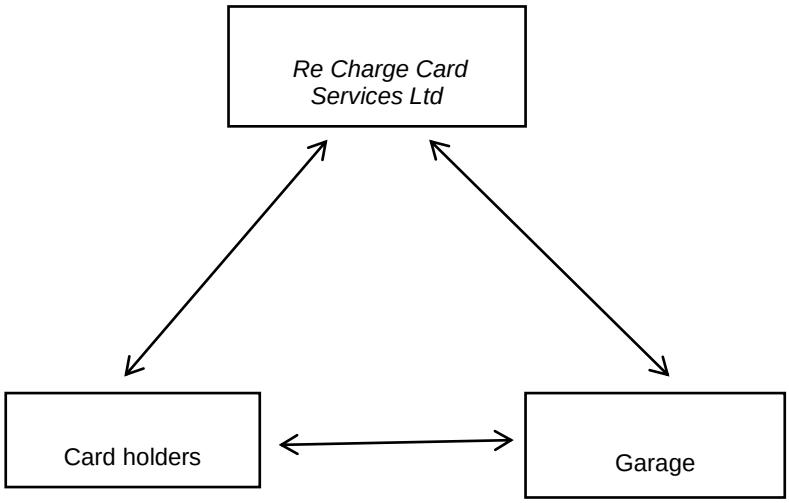
In this case, *Charge Card Services Ltd* ran a credit card scheme by which, under a subscription agreement, the card holder could obtain petrol and other services from approved garages and make payments with the charge cards issued by *Charge Card Services Ltd*. The card scheme operated as follows: under a master agreement the card holders obtained fuel or other services which were paid for by charge card and the use of signed vouchers. The garage would send the vouchers to the company for settlement. The card holders would then pay the company monthly for the goods and services they obtained.

[193] Smith and Robertson, *op.cit.,* at pp. 250-251.
[194] Re *Charge Card Services Ltd* [1987] 1 Ch.150.

The company provided the cardholders with goods and services. When the company went into liquidation it owed garages about £1.9 million. Consequently, some card holders owed monthly payments to the company. The liquidators collected about £2 million from the card holders. The problem was not who was responsible for the payment but whether it was the company or the garages which were entitled to the funds.[195] The case was disputed on the grounds of whether payment by credit card was absolute or conditional payment. Millett J. held that whether payment by card was considered absolute or conditional payment essentially depended on the contract between the holder and the seller. However, that contract did not explicitly cover this question. Moreover, Sir Nicolas Browne-Wilkinson V.C. held that there were three agreements: first, between the payee and the card issuer; second, between the payee and cardholder; and, finally, the agreement between the cardholder and the card issuer. In particular, the three agreements were based on the terms and conditions of the underlying agreement. So each agreement was independent of the others. In the contract between the payee and the cardholder, the payee takes no information from the cardholder, because the payee is certain that he would never return to the holder for the payment and claim only from the card issuer for payment. Therefore payment by credit cards are the same as payment in cash and function as absolute payment.[196]

[195] *Ibid.*
[196] *Re Charge Card Services Ltd* [1989] Ch. 497.

Figure 8: the Credit Card Schemes in *Re Charge Card Services Ltd.*



This point was disputed by counsel acting for the garages, who tried to establish that payment by credit card works as conditional payment in the same way as cheques. Counsel took the view that there was no general rule, so when the payment could not be transacted by a third party it would be considered as a conditional payment.[197] The court, conversely, held that, because there is prior agreement between the seller and card issuer, the card holder expected, when paying by credit card and signing the receipt, that the company or bank would be liable to the seller when it had received notice of the purchase. Sir Nicolas Browne-Wilkinson V.C. held:[198]

> "To my mind, all these factors point clearly to the conclusion that the transaction was one in which the garage was accepting payment by card in substitution for payment in cash, i.e. as an unconditional discharge of the price."

Accordingly, payment by credit card is equivalent to payment by cash, and thus the payee has no right to demand the cardholder for any risk, and demand the

[197] *Ibid.*
[198] *Ibid.*, at p. 513.

card issuer directly.[199] In this regard, if the card issuer becomes insolvent the payee has no right to request from the payer to pay, because it is not reasonable for the payer to pay twice; first to the card issuer due to the issuer-holder contract and second to the payee due to the issuer's insolvency. Furthermore, the payee agrees that payment by credit card is absolute that it is the card issuer's duty to make the payment.[200] Thus, before any EFT transactions a payer bears the risk of the insolvency of the paying bank, while, after the funds transfer transactions and compilation of payment, a payee bears the risk of the insolvency of the payee's bank. To achieve the purpose of this chapter, section 4.5 will aim to determine which party bears the risk of insolvency in the context of EFT transactions.

4.5 Allocating risk of EFT non-payment

The findings of this study suggest that the question of which party bears the risk of insolvency is best answered by considering first the time at which the EFT is regarded as completed and, secondly, the payment devices employed. The positive argument is that the payment instruction is executed when the payment is final, in the sense that there is no time or opportunity for a countermand, and this argument applies these rules on payment with reflections on suitable responses to the risk of payment provider insolvency. The present author considers that the EFT is completed for the payer when the payer's bank takes

[199] Cornelius, S., 'The legal nature of payment by credit card', (2003) 15 Mercantile Law Journal 153 at p. 159.
[200] Sayer, P. E, and Barrister, M. A., Credit Cards and the Law: An Introduction (1988, London, Fourmat), p. 8.

any action to execute the payment instruction. The author further considers that the EFT is completed for the payee when the payee's bank takes the decision to accept the payment orders on the payee's behalf. The reasoning behind this view is that the customer's bank (payer's bank and payee's bank) is chosen and appointed by the customers themselves. In this regard, it is reasonable for the law to allocate relevant risk to the customer who accepts the risk of his bank's solvency. Accordingly, the party which bears the risk of non-payment in EFT transactions should be as follows:

1. If the payer's bank accepted the payment instruction and debited the payer's account it bears a legal obligation for the benefit of the payee, as with transaction funds. The payee, in that case, has no right to request the payer to pay again in the event of the payer's bank's insolvency. By contrast, if the payer's bank did not accept the payment and afterwards became insolvent, the payer is liable to the payee for the transaction funds. In other words, before a payment transaction is made the payer bears the risk of his bank becoming insolvent.

2. If the funds transfer is credited to the payee's bank account and later the bank becomes insolvent, the payee's bank bears its insolvency and the payee cannot demand that the payer pays again. In other words after transfer of payment transaction, the payee bears the risk of the payee's bank's insolvency.

3. In banking practice, the duty of the payee's bank is to receive the fund transfer from the paying bank and credit it in the payee's account. Thus, in a case where the payer's bank debited the payer's account but the payee's bank defaults to collect the funds transfer from the payer's bank, and later the

payer's bank becomes insolvent, it would not be logical to say the payee's bank could impose on the payee the risk of the insolvency of the payer's bank, considering that the payee's bank was part of the payment transaction, which makes it owe a duty to the payee, and that there were sufficient controls to credit risk. Therefore it is not reasonable to accept the liberation of the payee's bank from the liability to the payee from the risk of the payer's bank's insolvency, since the payee did not choose or appoint the payer bank and therefore has no option but to accept the credit of the paying bank.[201]

4. When the payer's bank becomes insolvent between the time of accepting the payment order and debiting the payer's account but before the time of crediting the payee's account. Indeed, the payee's bank has a right versus the payer's bank as to when to credit the payee's account. But assuming there is agreement between the payer's bank and the payee's bank, establishing that if the payer's bank defaults before actually crediting the funds in the payee's account the payee's bank has no right versus the payer's bank, that clause would be unreasonable because the payee's bank cannot exempt itself from its duty of collecting the payee's fund from the payer's bank. In addition, there is no justification for absolving the payer's bank from the risk of insolvency and making the payee liable for such failure.[202]

The customer is not bound by any agreement between the banks unless the banker-customer agreement includes the terms and conditions established in the bank's agreement. Nevertheless, to protect the customer's rights any

[201] Rogers, *op.cit.,* p. 711.
[202] *Ibid.*, at p. 708.

unfair term in the agreement between the customer and the bank will be subject to the rules of the Unfair Contract Terms Act 1977, or the Unfair Terms in Consumer Contracts Regulations 1999.[203] These rules apply to ensure the lawfulness and equity of the standard terms and conditions of the banker-customer agreement. Thus, the customer has the right to depend on both the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contracts Regulations 1999 in case of any unfair terms and conditions. The Unfair Terms in Consumer Contracts Regulations 1999 enshrined that customers are under no obligation to comply with any unfair term in their agreements.

5. The payer's bank may use a correspondent or intermediary bank when it is incapable of transferring funds to the payee's account directly. In such cases, the correspondent or intermediary bank acts as agent to the payer's bank.[204] However, the problem arising with the intermediary bank's insolvency is as follows: assuming that a fund transfer transaction order is initiated but due to the insolvency of one or more of the correspondent or intermediary banks the funds transfer transaction is not final, which party involved in the EFT transaction will bear the risk of insolvency?

The correspondent or intermediary bank acts as agent to the payer's bank, thus, it is liable to execute the payer's bank instruction.[205] This fact will make the payer's bank bear the risk of the insolvency of the correspondent or intermediary banks, since it owes the paying bank an implicit contractual

[203] The Unfair Terms in Consumer Contracts Regulations 1999 (SI 1999/2083.
[204] *Calico Printers Association Ltd v Barclays Bank Ltd* (1931) 39 LI. L. Rep. 51.
[205] *Linklaters v HSBC Bank Plc* [2003] 2 C.L.C. 162; The same obligations apply between the payee's bank and the correspondent or intermediary bank.

obligation to take all reasonable care and skill. The paying bank in turn, as an agent to the customer, is liable to the payer for losses due to any defaults or negligence on the part of the correspondent or intermediary bank.[206] Furthermore, one of the paying bank's duties towards its customer is to refund any payment that it has not transacted. In modern practice, however, banks involved in funds transfer transactions and employing a correspondent or intermediary bank normally establish a term in their contracts with the customer stating that the correspondent or intermediary bank is employed at the customer's expense and risk. The customer has no right to pursue the intermediary bank because there is no privity in the contract between them and thus the intermediary bank owes no liability to the payer.[207] Exemption terms of this sort could be subject to an evaluation under the Unfair Contract Terms Act, 1977, and the Unfair Terms in Consumer Contracts Regulations, 1999, since both statutes cover all contractual terms that have not been subject to negotiation.[208] It is upheld within schedule 2 of the Unfair Contract Terms Act, 1977, that the banks have the right to include in their contracts with customers an express term excluding liability, but only if this term is deemed reasonable. Within these statutes, if the contract includes an 'unfair' term the customer shall not be liable for non-execution of that term.

[206] *Ibid.*
[207] *Calico Printers Association Ltd v Barclays Bank Ltd* (1931) 39 LI. L. Rep. 51 at p. 66 per Wright J. who held that there was no contractual relationship between the intermediary or correspondent bank and the customer, and thus there is no contractual liability even if the intermediary bank nominated in the contract between the customer and the payer's bank since such nomination creates no privity of contract between the customer and the intermediary bank. Also, see *Royal Products v Midland Bank* [1981] 2 Lloyd's Rep. 194 at p. 198 per Webster J. and in *Grosvenor Casinos Ltd v National Bank of Abu Dhabi* [2008] 1 C.L.C. 399 at [175].
[208] Unfair Terms in Consumer Contracts Regulations 1999, regulation 3(1).

Under the PSR 2009, the correspondent or intermediary bank has no liability to the payer bank in a case in which the payer gave the wrong information about the transaction[209] or in a situation of *force majeure*.[210] It seems that there are two significant differences between the common law and the PSR 2009 principals. First, under the PSR 2009, a correspondent or intermediary bank is liable if any default has been accrued and this is 'attributable' to the action of a correspondent or intermediary bank in carrying out the payment instruction, even if there is no wrong action in the execution of the payment instruction.[211] But it is not reasonable that the correspondent or intermediary bank bears the risk of non-execution of the payment order, even when there was no wrong action. However, the common law principle is, conversely, that the correspondent or intermediary bank has no liability to bear the risk of non-execution of the payment order unless it was negligent. Ellinger, et al. argue this point and explain that the correspondent or intermediary bank seems to be strictly liable under the PSR 2009,[212] because the PSR 2009 makes the correspondent or intermediary bank liable to the payer's bank for any losses when the payer's bank instruction is not executed, without looking to the reason for such defaults. Secondly, the common law principle determines the paying bank's rights for restitution from the bank that it ordered to act as its correspondent.

[209] PSR 2009, regulation 74.
[210] *Ibid*., regulation 69.
[211] *Ibid*., regulation 78.
[212] Ellinger, et al., *op.cit.,* p. 618.

4.6 Conclusion

Insolvency risk refers to the possibility of settlement not being passed at full value. The legal issues in EFT finality do not arise directly with funds transfers as long as payments are made and funds directly transferred. They arise when one of the banks involved in the transaction does not execute its obligation to make the payment. Payment is presumed to be final for the payer when the payer's bank obligates itself irrevocably to that payment, while payment is presumed to be final for the payee when the payee's bank obligates itself by accepting the payment. In this chapter it has been argued that a customer who opens an account with a bank necessarily bears the risk of that bank's insolvency. Thus the payer will be liable for the payment before the fund transfer transaction in the case of his bank's insolvency after the fund transfer transaction is made it is the payee who bears the risk of that insolvency.

One significant finding of this chapter is the existence of a need for a comprehensive legislative framework to regulate the rules and principles covering the risk of insolvency in EFTs within the banking system, thus replacing the practice of following precedents set by court cases. The advantage of formulating basic rules governing the finality of payment is their use in identifying the party which bears the risk of insolvency. The rules model suggested in this thesis[213] could be helpful in defining the finality of EFT's and in identifying the party which bears the risk of insolvency.

[213] See chapter seven, section 7.3.

Chapter Five

Privacy in the Context of EFT

5.1 Introduction

EFT systems deal principally with information in the form of a continuous exchange of banker-customer messages. The impact of EFT in this area has been both large-scale and efficacious. However, there have been concerns over confidentiality in the context of EFT, in relation to both the customer's financial affairs and the interests of the bank. There is also a problem as to whether banks employ adequate protection systems for keeping customers' information confidential and protecting electronic transactions. Further problems relate to liability and customer protection, particularly where a hacker gains entry to accounts. The chapter examines and analyses these problems in the light of the existing laws and proposes recommendations for future approaches to protection and disclosure of customer data in the EFT context.

The great concern about confidentiality in the EFT context compared with non-electronic payment systems is because, first, there are now numerous bank records full of customer information in the form of easily accessible electronic data. Secondly, electronic data in EFTs are easy to collect, organise and save and offer large amounts of information. Thirdly, the growth of EFT systems makes it possible in practice for banks to execute increasingly sophisticated analyses of their customers' financial affairs and saving and spending habits,

which enable banks to market their own products more effectively, but also provide a potentially very valuable source of information for third parties, such as Credit Reference Agencies (CRA's). One of the objectives of this chapter is to reflect the ambiguities surrounding the disclosure of customer data to CRA's and to investigate whether or not this disclosure is in the bank's interest. Fourthly, the internal procedures of EFT are invisible to customers who have no idea about the data collected about them, who is using that data, and for what purpose.

Banks have a duty of confidentiality to their customers and this duty is a necessary part of the banking system's requirements with regard to accuracy of information.[1] There are differences in the provision of confidentiality, which vary from one bank to another, depending on the terms and conditions detailed in the contract. On this basis, banking confidentiality has no rules common to all banks, hence a prevailing absence of unity and conformity. Nevertheless, confidentiality is an implied term in the banker-customer contract and it exists in order to prevent disclosures of customer data beyond the four permitted exceptions.[2] To achieve the purposes of this chapter, the bank's liability to protect customer's confidential information is divided into six main sections. The first four are devoted to an analysis and assessment of the rules applied in *Tournier v National Provincial Bank.*[3] Section 5.5 devotes to analysing the legal issues surrounding disclosure of customer credit data to the CRAs. Section 5.6 of this chapter is devoted to analysing the existing legal rules pertaining to

[1] Alqudah, F., 'Banks' duty of confidentiality in the wake of computerised banking', (1995) 10 *International Banking Law* 50 at p. 50.
[2] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461.
[3] *Ibid.*

confidential information in the EFT context. The section outlines the motive forces behind the application of the Data Protection Act 1998 and the Human Rights Act 1998 to the protection of customer data in the EFT context. Lastly, section 5.7 is devoted to determining which party bears the losses and damage resulting from breaches in the bank's duty of confidentiality in the EFT. This chapter demonstrates that the bank is liable to the customer for any losses or damage resulting from disclosures of confidential information or data without legal provision or beyond what is justified by law. In contrast, the customer is shown to be liable for any disclosure due to his negligence or approval. The conclusion reached is that the *Tournier* principles fail to provide a sufficient remedy when applied to the bank's duty of confidentiality in the EFT context. Further, there is a lack of uniform or harmonized legislation regarding arrangements for data exchange in an EFT context. The model rules suggestions in this thesis could be of help in regulating a bank's duty of confidentiality in the EFT context. [4]

5.2 The legal nature of confidentiality

The EFT banker-customer relationship is an agency contract, thus the nature of privacy [5] stems from this contract. Generally, an agent is under a duty of confidentiality to his principal. [6] Diplock L.J. in *Parry-Jones v Law Society* [7]

[4] See chapter seven, section 7.4.
[5] For the meaning and defining privacy term, see Koutsias, M., 'privacy and data protection in an information society: who reconciled are the English with the European union privacy norms?', (2012) 18 *Computer and Telecommunications Law Review* 261 at pp. 262-267.
[6] *Regal (Hastings) Ltd v Gulliver* [1967] 2 A.C. 134; *Boardman v Phipps* [1967] 2 A.C. 46.
[7] *Parry-Jones v Law Society* [1969] 1 Ch.1 at p. 9.

explained the duty of confidentiality between the agent and his principal, Diplock L.J. held:

> "What we are concerned with here is the contractual duty of confidence, generally implied though sometimes express, between a solicitor and client. Such a duty exists not only between solicitor and customer, but, for example, between banker and customer, doctor and patient and accountant and client. Such a duty of confidence is subject to, and overridden by, the duty of any party to that contract to comply with the law of the land. If it is the duty of such a party to a contract, whether at common law or under statute, to disclose in defined circumstances confidential information, then he must do so, and any express contract to the contrary would be illegal and void."[8]

There are two motivations for the agent's duty of confidentiality, economic and historic.[9] Both these motivations justify the obligation of confidentiality in the banker-customer contract. First the economic motivation. From the customers' viewpoint, a duty of confidentiality encourages them to involve others in their businesses, given that such an obligation will protect them from unjustified external attempts to investigate their business or commercial secrets, and confidentiality therefore may persuade them to enter an especially competitive area of trade in which they might not otherwise have been involved.[10] From the agents' viewpoint, on the other hand, there are some types of business that could not be completed unless the principal discloses some information. The contract of lawyer and client well demonstrates such a point.[11] Thus the economic motivation justify the duty of confidentiality in the banker-customer relationship, for example, an individual is encouraged to involve into a banking agreement by the fact that he may conduct his business dealing with the bank secreted family or commercial competitors; and the services that the bank

[8] *Ibid.*, at p. 9
[9] Reynolds, F.H.B., *Reynolds on Agency* (2001), para. 6-032.
[10] *Ibid.*
[11] Ellinger, E., et al., *Modern Banking Law* (2011), p. 172.

supplies are subjected to the fact the customer in more willing to disclose his financial information if this is done on a confidential ground. Historically, the agent always attempts to gain the customer's trust.[12]

Confidentiality is of such a nature that it is implicit, and begins the moment the banker-customer relationship is initiated. This point is well documented in *Tournier v National Provincial Bank*[13] when the Court of Appeal held that the bank's commitment to maintaining confidentiality regarding the affairs of the customer is a legal and moral obligation arising from an implied term in the banker-customer contracts.[14] Prior to *Tournier* a duty of confidentiality was considered a moral duty only. In the banking sector, banks seeking to make a profit amid intense competition depend on their reputation and need to attract customers by inspiring confidence in their activities if they are to optimize their profits. However, the bank's obligation of confidentiality is a legal one, and most banks have recently started to include in their contracts with customers terms dealing with confidentiality under different titles, for example, the use of information about customers,[15] personal information,[16] or confidentiality.[17] Thus, confidentiality is currently an explicit legal term in many banker-customer contracts.

---

[12] Alhosani, W., 'Banking Confidentiality Against Disclosure', (2012) *Durham Law Review* 1 at p.3 http://durhamlawreview.co.uk/files/Banking_confidentiality_against_disclosure.pdf 20 August 2012.

[13] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461.

[14] *Ibid.,* at pp. 471-472.

[15] Barclays, *Barclays Terms: Your Agreement with Us,* 2013, section G http://www.barclayswealth.co.uk/Images/IBIM1000.pdf 22 April 2013.

[16] Lloyds TSB, *Personal Banking terms and conditions,* 2012, section D (14) http://www.lloydstsb.com/media/lloydstsb2004/pdfs/personal_banking_terms_and_conditions.pdf 6 April 2013.

[17] HSBC, *General Terms and Conditions, Current Accounts Terms and Conditions,* 2012*,* section 2(34)[34.2] http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf 6 April 2013.

5.3 Ambit, duration, and termination of the bank's a duty of confidentiality

It is an observable fact that the bank's duty of confidentiality is activated from the moment a banker-customer contract is initiated as, for example, by the opening of a bank account. There is no banker-customer relationship before the opening of a bank account.[18] Further, there is no duty of confidentiality to non-customers regarding the information obtained from the negotiations between the bank and an individual where no contract has been signed. There is a duty of confidentiality to non-customers, however, when the bank presents an express obligation to keep the information secret. Accordingly, in the EFT context the question arising is whether a bank's duty of confidentiality is protected and limited to information obtained from the customers and their account or whether it extends to information obtained from any sources other than the customers or their account.

The answer to this question has two aspects. The first was expressed in *Tournier* by Bankes L.J. and Atkin L.J. who held that the bank's duty of confidentiality covered all customers' information about themselves and their accounts obtained by the bank, irrespective of the information source and for as long as the banker-customer relationship existed.[19] In contrast, Scrutton L.J. held that the bank's duty of confidentiality is limited to account transactions information only, and that the duty did not cover any information received by the

[18] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461 at p. 481 per Scrutton L.J.
[19] *Ibid.,* at pp. 473-474 per Bankes L.J. and p. 485 per Atkin L.J.

bank from sources other than its customers or their account transactions.[20] In fact, the present author agrees with the first view, the same view held by the Court of Appeal, which is authoritative and reasonable due to the fact that the information is given to the bank in regard to the contractual agreement between the bank and the customer.

That aspect of a bank's duty of confidentiality exists if there is a contractual agreement between the bank and the customer.[21] However, there is also the question of information received by the bank before the initiation of such a contract. The answer is provided by *Tournier.* The first view was put forward by Bankes L.J. and Atkin L.J., who held that the bank's duty of confidentiality does cover the information received by the bank before the beginning of the banker-customer contract.[22] Scrutton L.J. held a contrary view arguing that the bank's duty of confidentiality does not cover this information.[23] Nevertheless, there is agreement that the bank's duty of confidentiality does not extend to the information received after termination of the banker-customer contract.

Given the above exposition, it seems that there are many reasonable and logical reasons for obliging the banks to keep customers' confidential data private before, during, and after their relationship. These reasons are: first, information provided to the bank before beginning the contractual agreement is possibly the same information that is provided by the customer after beginning

[20] *Ibid.,* at p. 481-482 per Scrutton L.J.
[21] *Barclays Bank Plc v Taylor* [1989] 1 W.L.R. 1066 at p. 1070, Lord Donaldson M.R. held: "The banker-customer relationship imposes upon a bank a duty of confidentiality in relation to information concerning its customer and his affairs which it acquires in the character of his banker.".
[22] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461 at pp. 473-474 per Bankes L.J. and p. 485 Atkin L.J.
[23] *Ibid.,* at p. 481 per Scrutton L.J.

the contractual agreement; consequently such information falls under the duty of confidentiality. Secondly, information provided to the bank at any period during the banker-customer relationship does indeed fall under the bank's duty of confidentiality according to the common law definition of confidence.[24] Thirdly, in practice, there is nothing to prevent banks from assuming an explicit duty to the customer to inhibit the disclosure of specific information, even if such information theoretically is not within the ambit of the bank's duty of confidentiality. Fourthly, the customer's right of privacy must certainly be respected and a most important aspect of the person's right is the right to keep his information private. Therefore, there is a possibility that disclosure of any confidential information after the termination of the banker-customer relationship causes loss or damage to the person.[25] Finally, customer's confidential information could be commercially sensitive and the customer would not wish for disclosure because his new business could be adversely influenced by such information. The present author's view is that the bank's duty of confidentiality should be kept indefinitely, even after the customer's death, as long as the law does not indicate a specific time for the termination of the duty.

According to *Tournier*, the implied duty of confidentiality exists if there is a contractual agreement between the bank and the customer. However, in the EFT context, banks supply their customers with a wide range of transactions services going well outside the classical functions of deposit-taking and lending, and often not all transactions include a contract between the bank and a particular person, for instance when the creditor has an account in another

[24] *Attorney-General v Guardian Newspapers Ltd (No. 2)* [1990] 1 A.C. 109 at p. 281-282 per Lord Goff.
[25] Hapgood, M., *Paget's Law of Banking* (2007), p. 158.

bank. There may be no express term from the bank to the person to keep the information secret, and so there is no duty of confidentiality, and therefore the problem exists as to whether the bank's implied duty of confidentiality covers information that it obtains when acting beyond its classical deposit-taking role.[26] Therefore, it seems that this problem can be answered only by addressing the bank's duty of confidentiality within the general rules of breach of confidence, rather than by covering the bank's duty of confidentiality by a separate area of law.[27] In *Attorney-General v Guardian Newspapers Ltd (No. 2)* Lord Goff[28] addressed the general rules covering breach of a duty of confidentiality, where Lord Goff held:

> "A duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others….To this broad general principle, there are three limiting principles to which I wish to refer. The first limiting principle…is that the principle of confidentiality only applies to information to the extent that it is confidential… The second limiting principle is that the duty of confidence applies neither to useless information, nor to trivia… The third limiting principle is of far greater importance. It is that, although the basis of the law's protection of confidence is that there is a public interest that confidences should be preserved and protected by the law, nevertheless that public interest may be outweighed by some other countervailing public interest which favours disclosure." [29]

It seems that Lord Goff's approach is comprehensive, and there is no obstacle to making this approach cover the bank's duty of confidentiality.[30] Generally, the confidant's liability for breach of confidential information exists by virtue of a

[26] Cranston, R., *Principles of Banking Law* (2002), p. 171-174; Ogilvie, M. H., 'From secrecy to confidence to the demise of the banker customer relationship: *Rodaro v Royal Bank of Canada*', (2003) 19 *Banking and Financial Law Review* 103 at pp.112-113.
[27] *Ibid.*
[28] *Attorney-General v Guardian Newspapers Ltd (No. 2)* [1990] 1 A.C. 109 at p. 281-282.
[29] *Ibid.*, at p. 281-282.
[30] Ellinger, et al., *op. cit.,* p. 179.

general equitable obligation imposed by the law on the confidant towards the confider, rather than by means of a term implied in the banker-customer contract. It presents a legal source for protecting confidential information disclosed to a bank by a customer in a non-banking context, for example, when a bank offers investment advice or asset management services, or by a non-customer, for example, when presenting a business plan to secure bank finance.[31] Nevertheless, Ellinger et al. argue that 'it is difficult to set general rules covering breach of confidence with the scope of the implied duty recognized in *Tournier*, since each recognize different circumstances in which confidential information may be revealed'.[32]

A bank's duty of confidentiality is not an absolute, it exists in varying degrees and the most fundamental secrets can be waived in cases where the law allows.[33] *Tournier* identified four circumstances where the bank has the right to disclose its customer information.[34] Bankes L.J. held that:

> "On principle I think that the qualifications can be classified under four heads: (a) Where disclosure is under compulsion by law; (b) where there is a duty to the public to disclose; (c) where the interests of the bank require disclosure; (d) where the disclosure is made by the express or implied consent of the customer."[35]

[31] *Ibid.*
[32] *Ibid.*
[33] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B; Further, see Haynes, A., *The Law Relating to International Banking* (2010), pp. 166-167.
[34] *Ibid.,* p. 473 per Bankes L.J.
[35] *Ibid.,* p. 473 per Bankes L.J.

5.4 Qualifications and exceptions to the duty of confidentiality

5.4.1 Disclosure by compulsion of law

Recently there has been an increased amount of legislation authorizing courts to order the inspection and revelation of bank documents or otherwise requiring bank disclosure in specific circumstances, adding more exceptions to the bank's duty of confidentiality.[36] Court proceedings are the best example of an obligation by law,[37] for example, when a bank is ordered to disclose information about its customer's account during the legal proceedings.[38] In *Bucknell v Bucknell*[39] and *Eckmam v Midland Bank Ltd*[40] the court ordered the bank to disclose information about its customer's account in favour of the public interest and the administration of justice. When the court orders the bank to disclose customer information, the bank can do so without obtaining the customer's consent.

A bank must submit information and documents required by the court and cannot refuse on the basis of confidentiality because refusing to respond to the court's order would render the bank in contempt of court.[41] For instance,

[36] Ogivie, M. H., 'Banker and customer: the five-year review 2000-2005', (2007) 23 *Banking and Finance Law Review* 107 at p. 144; *Report by the Review Committee on Banking Services: Law and Practice*, ("The Jack Report") (1989, London, HMSO, Cm 622), p. 30. This chapter will not consider all these regimes, but it will focus on the most common examples relating to the banker-customer relationship.
[37] Charles, P., *The Law and Practice of International Banking* (2010), p. 681.
[38] Alastair, H., *The Law of Finance* (2009), p. 779.
[39] *Bucknell v Bucknell* [1969] 1 W.L.R. 1204.
[40] *Eckmam v Midland Bank Ltd* [1973] Q.B. 519.
[41] Ross, C., *Principles of Banking Law* (2002), p. 176.

pursuant to the jurisdiction recognized in *Norwich Pharmacal Co v Customs and Excise Commissioners*,[42] a bank may be obliged to make pre-action disclosure of confidential information about its customer to a third party who needed that information in order to build his case against the customer. However, in *Mitsui & Co Ltd v Nexen Petroleum UK Ltd*,[43] the court required three conditions to grant a *Norwich Pharmacal* order:

> "The three conditions to be satisfied for the court to exercise the power to order Norwich Pharmacal relief are: i) a wrong must have been carried out, or arguably carried out, by an ultimate wrongdoer;
> ii) there must be the need for an order to enable action to be brought against the ultimate wrongdoer; and
> iii) the person against whom the order is sought must: (a) be mixed up in so as to have facilitated the wrongdoing; and (b) be able or likely to be able to provide the information necessary to enable the ultimate wrongdoer to be sued."[44]

According to *Norwich Pharmacal* the following conditions are required: first, a wrongful action must have been committed;[45] secondly, an order must be necessary to enable action to be brought against that wrongdoer; and thirdly, the person against whom the order is required must be 'mixed up' in the acts of the wrongdoer so as to have facilitated the wrongdoing and be able to supply the significant information for that wrongdoer to be sued. With regard to the third condition, banks are possibly to become innocently mixed up in their customer's wrongdoing, such as income from an unauthorized transaction passing through

[42] *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] A.C. 133 at p.175.
[43] *Mitsui & Co Ltd v Nexen Petroleum UK Ltd* [2005] EWHC 625 (Ch) per Lightman J.
[44] *Ibid.,* at para. [21] per Lightman J.
[45] Regardless, whether a wrongdoer involves civil or criminal liability, see *Ashworth Hospital Authority v MGN Ltd* [2002] 1 W.L.R. 2033 at [34-35] and [53].

that account,[46] and consequently banks are mostly subject to the *Norwich Pharmacal* jurisdiction.[47]

A similar application of the *Norwich Pharmacal* jurisdiction to the banking context can be found in *Bankers Trust Co v Shapira,*[48] although this case has been clarified as subject to the exercise of a distinct, but connected, jurisdiction.[49] In this case two fraudsters obtained a substantial sum of money by introducing to the bank in New York cheques allegedly drawn on it by a bank in Saudi Arabia. The bank passed the money relating to the cheques to the perpetrators of the fraud by whose order the money was to be transferred to their account in the bank in London. When the cheques were found to be forgeries the bank in New York paid back the money debited to the account of the Saudi Arabian bank and attempted to recover its losses from the two culprits. In an attempt to find them, the bank asked for an order instructing the defendant's bank to authorize the bank to check and take copies of all documents, including the cheques transacted in that account between the fraudsters and the defendant's bank. Mustill J.[50] refused to grant this order. His reasoning was that the culprits had not been found and that it would be, in any case, a mistake to give such an instruction at the interlocutory stage. In overturning this decision, the Court of Appeal did however hold that the court must be very careful when ordering a bank to disclose data from its customer's account and the documents and correspondence relating to it, as it was "a

[46] Ellinger, et al., *op.cit.,* p. 181.
[47] *Koo Golden East Mongolia v Bank of Nova Scotia* [2008] Q.B. 717 at pp. 731-733, per Sir Anthony Clarke MR who held that the *Norwich Pharmacal* jurisdiction is likely to be particularly useful against banks when seeking information to assist in tracing the proceeds of fraudulent or criminal activity.
[48] *Bankers Trust Co v Shapira* [1980] 1 W.L.R. 1274.
[49] Ellinger, et al., *op.cit.,* p. 182.
[50] *Bankers Trust Co v Shapira* [1980] 1 W.L.R. 1274 at pp. 1274-1275.

strong thing to order a bank to disclose the state of its customer's account and the documents and correspondence relating to it".[51] Such an order should be granted only if there is reasonable and good evidence that the money in the bank is the plaintiff's money.[52] Therefore, mandatory revelation substituted for the customer's consent. Furthermore, the bank was under no obligation to notify its customer that revelation has been made, since a notification may have obstructed any investigation.

Furthermore, in *Arab Monetary Fund v Hashim,*[53] Hoffmann J. emphasised two more conditions that have to be considered, by the court, before creating a *Norwich Pharmacal order*: first, the order must be for specific information or documents; and secondly, the court has to strike a balance between the duty of confidentiality and the disclosure of information order.[54] From the bank's viewpoint, although such an order for information disclosure would be legitimate in order to protect a bank from legal action for breach of duty of confidentiality in the local courts, a bank might not have similar protection abroad.[55] Therefore most banks initiated the practice of protecting themselves by including a general term in their contract with the customers enabling the bank to disclose customer data where it was legally required to do so.[56]

The author view is that granting an absolute order to disclose private customer information or documents is an unfair practice. Therefore, the court must take into account when issuing the order the scope and limitations of such an order.

---

[51] *Ibid*., at p. 1282 per Lord Denning M.R.
[52] *Ibid*., at p. 1282.
[53] *Arab Monetary Fund v Hashim (No.5)* [1992] 2 All E.R. 911.
[54] *Ibid.,* at p. 919.
[55] *Ibid*. at p. 920.
[56] HSBC, *General Terms and Conditions, op.cit.,* [34.2].

In this regard, all the documents and the evidence which the bank has the right to disclose must be relevant to the case that is subject to dispute. Thereby, under the Civil Procedure Rules1998[57] (CPR hereafter), at the moment that the information is revealed in the court it will constitute public information.[58] Nevertheless, it is appropriate that the court has the right to issue an order restraining and prohibiting the use of the information disclosed.[59]

The CPR 1998, Part 34, presents a new procedure in which the court has the right not only to disclose private information but also to create a 'witness summons'.[60] A 'witness summons' means the right of the court to order a person to attend the court as a witness and to present all the evidence and documentation which could influence the court's decision.[61] Furthermore, the CPR 1998 rule 31.18 presented a new system whereby a victim has the right to obtain disclosure of documents against a person who is not a party to proceedings before proceedings have started.[62] Griffiths[63] argues that the order application must clarify with reasonable particularity the documents or identifiable categories of documents to be presented'.[64] Nonetheless, in practice, a court is very careful when exercising its discretion to create a witness summons or issue an order to enforce parties to reveal information. A

[57] Civil Procedure Rules 1998 (SI 1998/3132) (L.17). CPR 1998 is applied the *Norwich Pharmacal* jurisdiction, as neither the pre-action disclosure rule in CPR 1998, rule 31.16, nor the third party disclosure rule in CPR 1998, rule 31.17, applies to per-action disclosure against non-parties to the relevant proceedings. Hollander, C., Documentary Evidence (2012), para. [5-35].
[58] CPR 1998, rule 31.22 (1).
[59] *Ibid.*, rule 31.22 (2).
[60] *Ibid*., rule 34.2(1); Further, see Baker, D., and Anstey, N., 'Disclosure of Documents' in Blair, W., *Banks and Remedies* (1999), Ch. 4.
[61] *Inner West London Assistant Deputy Coroner v Channel 4 Television Corporation* [2008] 1 W.L.R. 945.
[62] *Fanmailuk.com Ltd v Cooper* [2010] EWHC 2647 (Ch); See also Riem, A., 'To catch a cyber thief: tracing internet crime', (2007) 184 *The In-House Layer* 43 at p. 44.
[63] Griffiths, G., *Neate, Bank Confidentiality* (2008), p. 257.
[64] *Ibid.*

fortiori, courts must be very careful when exercising such discretion and the same care should be exercised with regard to any third party who is a non-party in the case.[65]

Section 7 of the Bankers' Books Evidence Act 1879 presents another qualification to the bank's duty of confidentiality, although a distinction is made between civil and criminal procedures. The Bankers' Books Evidence Act 1879 section 7 states:

> "on the application of any party to a legal proceeding a court or judge may order that such party be at liberty to inspect and take copies of any entries in a banker's book for any of the purposes of such proceedings."

'Legal proceedings' may mean either civil or criminal proceedings. Civil proceedings fall under the Civil Evidence Act 1995, and the CPR part 33. These regimes allow for the admission of hearsay evidence, including statements contained in documents [66] and business reports, [67] as evidence in civil proceedings. Additionally the Criminal Justice Act 1988 allows for hearsay documentation to be taken as evidence in criminal proceedings, regardless of the source from which it issues.

In legal proceedings the court has the right to authorize an inspector to obtain any copies of the bank's records.[68] The bank however has a right to a period of time in which to prepare required documents and in such a period the bank may

[65] *Robertson v Canadian Imperial Bank of Commerce* [1994] 1 W.L.R. 1493; Also, see European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 article 8 came into force in 2000, in such article the Convention giving a right to protect and respect persons' privacy
[66] Civil Evidence Act 1995, section 8.
[67] *Ibid*., section 9.
[68] Ibid., section 9(2) defines 'bankers' books' to include ''ledgers, day books, cash books, account books and other records used in the ordinary business of the bank, whether those records are in written form or are kept on microfilm, magnetic tape or any other form of mechanical or electronic data retrieval mechanism.''.

exercise the right to object.[69] When a bank is asked in suitable and acceptable cases to supply their relevant records of customers' information, such records will be considered as evidence in the case.[70] Recently, and with EFT transactions, customers' data are recorded electronically and submitting such data will be by making an electronic copy (CD) which the court could consider sufficient evidence.[71] On this basis, Hollander[72] agrees that: "it is obvious that the use of the Bankers' Books Evidence Act 1879 has progressively been marginalized by development of civil and criminal procedures."

Electronic and internet information records fall under section 9 (2) of the Bankers' Books Evidence Act 1879. Thus, the courts have the right to grant an order to obtain copies of these types of electronic banking data records. Nevertheless, the EFT system makes it very hard to disclose the original copy of an electronic datum and therefore these disclosures would very likely be compiled orally, or in an affidavit attached to a copy of the data record required. Moreover, not all of a bank's documents fall under the Bankers' Books Evidence Act 1879. Documents that are not addressed by the bank's data, for example, messages to the bank's customer,[73] invalid cheques and errors of credit,[74] are not classified as 'Bankers' Books'.

---

[69] *DB Deniz Nakliyati TAS v Yugopetrol* [1992] 1 W.L.R. 437.

[70] For electronic data as an evidence generally, see Tapper, C., 'Evidence from computer', (1975) 4 *Rutgers Journal Computer & Law* 324; Tapper, C., 'Evidence and computers', (1984) 101 *South African Law Review* 675; Tapper, C., 'Discovery in modern crimes: a voyage around the common law word', (1991) 67 Chicago-Kent Law Review 217; Collins, V., 'Computerised Evidence: Finding the Right Approach', (1994) 3 *Nottingham Law Journal* 11; Chung, C. S., and Byer, D. J., 'The electronic paper trail: evidentiary obstacles to discovery and admission of electronic evidence', (1998) 22 *Journal of Science & Technology Law* 1.

[71] *Ibid.*

[72] Hollander, C., *Documentary Evidence* (2012), para.5-42.

[73] *Re Howglen Ltd* [2001] B.C.C. 245 at p. 246 the court held that: "in the present case were essentially the records of meetings which could not be properly regarded as entries in the bank's books for the purpose of its ordinary business.".

The banks have no power to avoid the courts order and so they must disclose customer information in accordance with the compiled statutes. This chapter will examine the most important statutes associated with banker-customer relationship.

5.4.1.1 Money laundering[75] and the financing of terrorism

EFT systems constitute the best environment for money 'launderers' when parties transfer funds from one bank account to another.[76] Due to the great expansion of banking services offered by EFT transactions, funds transfers from one country to another have become very easy and very fast. Money launderers also take advantage of banking confidentiality which may protect the perpetrators of organised crime. EFT transactions have recently been associated with a number of crimes, such as money laundering, drugs trafficking and terrorism.[77] This has led to the establishment of a number of statutes to control and deal with such crimes. These regulations are: the Proceeds of Crime Act 2002; the Money Laundering Regulations 2007;[78] and the Terrorism Act 2000. These legislations place important impositions on the bank by allowing disclosure of customers' information when suspicious activities

[74] *Williams v Barclays Bank Plc* [1988] Q.B. 161 at p. 163; *Volkering and others v District Judge Haughton and another* [2005] IEHC 240.
[75] Laundering or money laundering means the actions taken by an individual to hide the true source of the money they got from the practice of illegal activities, or is trying to give the character of legitimacy to the money earned from the commission of crimes and activities. This action constitutes against the law, see Hudson, A., *The Law of Finance* (2009) p. 337.
[76] Turner, J. E., *Money Laundering Prevention* (2011), pp. 91-92.
[77] Ellinger, et al., *op.cit*., Ch.4.
[78] Money Laundering Regulations 2007 (SI 2007/2157) amended by (SI 2007/3299), the PSR 2009 (SI 2009/209), The Money Laundering (Amendment No.2) Regulation 2011 (SI 2011/2833), and (SI 2012/2298).

occur within customer transactions.[79] These statutory instruments place the person (bank) under an obligation to report any operations that are suspected of involving money laundering or other suspicious activities.[80] Not reporting such activities places the person (bank) in breach of legal provisions.[81] These exceptions grant the bank the right to breach its duty of confidentiality.[82]

The Money Laundering Regulations 2007 impose on the bank different obligations respecting the control, reduction and detection of money laundering and the financing of terrorism.[83] The first obligation is for the bank to take on the routine duty of investigating its customers and their actions after they open an account and for the period of its operation, such actions being called 'customer due diligence measures'.[84] The bank is obligated to apply 'customer due diligence measures' in the following cases: when the customer opens an account, which normally initiates a banker-customer contract;[85] when the transaction amount exceeds 15,000 Euros;[86] and where there is any suspicion that the transaction involves money laundering.[87] Such provisions allow banks to participate in the maintenance and protection of the financial system in general. Furthermore, since one of the bank's duties is to exercise all reasonable care and caution, then if it registers any out of the ordinary transactions it should examine the indications of suspicious activities and

[79] Section 328 of the Proceeds of Crime Act 2002; Part III of the Terrorism Act 2000 and the Money Laundering Regulations 2007.
[80] Haynes, A., 'Money laundering: from failure to absurdity', (2008) 11 (4) *Journal of Money Laundering Control* 303 at p. 305.
[81] *Ibid.*
[82] *Tayeb v HSBC Bank plc* [2005] 1 C.L.C. 866 at p. 871.
[83] Money Laundering Regulations 2007, regulation 20.
[84] *Ibid.,* regulation 7(3).
[85] *Ibid.,* regulation 7(1)(a).
[86] *Ibid.,* regulation7(1)(b); occasional transaction is defined under regulation 2(1) as "a transaction carried out other than as part of a business relationship".
[87] *Ibid.,* regulation 7(1)(c).

monitor the movement of suspect funds.[88] Secondly, the bank must save the customer data for no less than five years after the customer relationship is terminated.[89] However, not all customer data are required to be kept on record, only the documents referring to the customer's identity,[90] and data subject to a business relationship or occasional transactions which are the subject of customer due diligence measures or on-going monitoring.[91] Thirdly, the bank is obligated to have 'risk-sensitive policies and procedures', in all its operations.[92] Fourthly, the bank is under an obligation to train its employees in the skills and knowledge necessary for the identification of transactions which may involve money laundering or terrorist financing.[93] Any bank which fails to fulfil these obligations falls under legal accountability, through either civil or criminal liability.[94] It should be noted that under the 2007 Regulations the bank is liable to report the customer's suspect transaction even if a crime did not in fact take place.

The author's view is that, while the 2007 Regulations represent an attempt to reduce or control the crime of money laundering by imposing on the bank several obligations, such obligations create a problematical conflict between the bank's duty of confidentiality and its obligation to inform the legal authorities of any suspicions of money laundering or terrorist financing.[95] Within these provisions a bank must report any suspicions of criminality in the customer's

[88] *Ibid.,* regulation 15.
[89] *Ibid.,* regulation 19.
[90] *Ibid.,* regulation 19(2)(a).
[91] *Ibid.,* regulation 19(2)(b).
[92] *Ibid.,* regulation 20.
[93] *Ibid.,* regulation 21.
[94] *Ibid.,* respectively regulations 42 and 45.
[95] Section 337 of the Proceeds of Crime Act 2002 protects the bank for any disclose and section 338 authorised disclosures.

transactions, otherwise it will be under liability for not reporting the crime of money laundering. In practice, there is normally an explicit term in the banker-customer contract that allows the bank to disclose confidential customer information in order to prevent crime, irrespective of whether the disclosure takes place in the UK or abroad.[96] In addition there is an implied term in the banker-customer contract allowing the bank to reject execution of a payment instruction where suspicious activities are referenced in the transaction.[97] In normal practice the bank would not report any suspicious activities on the part of their customers unless they have obtained an order from the court ordering them to disclose their confidential customer data. Even if there are suspicious activities, the bank may not report those activities to the legal authorities, justifying such a course by claiming that it did not discern criminality in the customer's transaction. In some cases, however, the bank may disclose its customer data, claiming that since there was suspicious activity it bore no liability for any such disclosure. The author's view therefore is that there is a need to draw boundaries in order to determine exactly when the bank has the right to exchange customer data. That boundary could be when there is clear, certain and sufficient evidence that the customer's transaction involves criminal activities.

[96] Barclays, *Barclays Terms:* Your *Agreement with Us 2013*, section G [4] http://www.barclayswealth.co.uk/Images/IBIM1000.pdf 22 January 2013; Lloyds TSB, *Personal Banking terms and conditions, October 2012*, section D 14 [14.10.](b) http://www.lloydstsb.com/media/lloydstsb2004/pdfs/personal_banking_terms_and_conditions.pdf 6 October 2012; HSBC, *General Terms and Conditions, Current Accounts Terms and Conditions, April 2012,* section 2(34)[34.5.2] http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/uk/pdfs/en/General_Current_Accounts_Aprl1.pdf 6 October 2012.

[97] *Shah v HSBC Private Bank (UK) Ltd* [2013] Bus. L.R. D38.

5.4.1.2 Disclosure of confidential information to tax authorities

A bank is under a duty to disclose confidential information relating to its customers when ordered to do so by the court in accordance with tax legislation. Examples of the relevant legislation are: sections 13, 17, 20 and 24 of the Taxes Management Act 1970, section 745 of the Income and Corporation Taxes Act 1988, and section 771 of the Income Tax Act 2007. According to these statutes the bank is obliged to submit a statement to the legal authorities that the financial profit or income of its customer is taxable. In this regard, a bank is under no duty of confidentiality when disclosing its customer's confidential information compiled according to the tax authorities' order, and there is no breach of the contract with the customer. Section 17(1) of the Taxes Management Act 1970, establishes that every person carrying on the trade or business of banking is obliged to disclose if required to do so by notice from a tax inspector. Correspondingly, if there is no order for disclosure the bank is under no duty to disclose confidential information and any disclosure would be in breach of the contract and its duty of confidentiality, any such breach placing the bank under a liability. The general approach of the UK tax authorities is to obtain information from the bank on its customers for tax purposes by ordering the bank via the court to present particular information and documents pertaining to the tax cases of particular taxpayers. However, in the UK the legal tax authorities are required to follow a specific procedure in requesting a bank to disclose confidential information. This procedure requires the agreement of

an independent commissioner.[98] One question that might have to be considered is: if the bank suspected that one of its customers was seeking to evade tax liabilities would it be obliged to disclose information to the tax authorities?

As explained above, the Proceeds of Crime Act 2002 place important impositions on the bank by allowing disclosure of customers' information when suspicious activities occur within customer transactions.[99] Section 338 places the person (bank) under an obligation to report any operations that are suspected of involving criminal activities.[100] Not reporting such activities places the person (bank) in breach of legal provisions.[101] These exceptions grant the bank the right to breach its duty of confidentiality.[102] In *K Ltd v National Westminster Bank Plc.*[103] In such case the court held that a disclosure by a banker to the authorities that he suspects he is being asked to facilitate the use or control of criminal property is an authorised disclosure pursuant to section 338 of the Proceeds of Crime Act 2002.[104] Furthermore, as explained above, Money Laundering Regulation 2007 impose essential obligation on the bank by allowing disclosure of customers' information when suspicious activities occur within customer transactions.[105]

[98] Taxes Management Act 1970, section 2.
[99] The Proceeds of Crime Act 2002, sections 237-328.
[100] Haynes, A., 'Money laundering: from failure to absurdity', (2008) 11 (4) *Journal of Money Laundering Control* 303 at p. 305.
[101] *Ibid.*
[102] *Tayeb v HSBC Bank plc* [2005] 1 C.L.C. 866 at p. 871; *K Ltd v National Westminster Bank Plc* [2007] 1 WLR 311.
[103] *K Ltd v National Westminster Bank Plc* [2007] 1 WLR 311.
[104] *K Ltd v National Westminster Bank Plc* [2007] 1 WLR 311, at p. 316.
[105] Sections 327-328 of the Proceeds of Crime Act 2002; Part III of the Terrorism Act 2000 and the Money Laundering Regulations 2007.

In *R. v Da Silva*[106] the term suspicion was defined as 'a word that can be used to describe a state-of-mind that may, at one extreme, be no more than a vague feeling of unease and, at the other extreme, reflect a firm belief in the existence of the relevant facts'.[107] Although, the court held that in order for there to be "blind-eye" knowledge, a vague feeling of unease is not enough but suspicion must be "clear" or "firmly grounded and goal on particular facts", or depend on "reasonable grounds".[108] Thus, a bank must report any suspicions of criminality in the customer's transactions otherwise it will be under liability for not reporting.

5.4.1.3 Part XI of the FSMA 2000

The FSMA 2000[109] granted the Financial Conduct Authority powers to require the bank to reveal confidential information relating to its customers.[110] The purpose of that right is to build upon communications with customers, which requires a bank to pay due regard to their data needs. This helps in the achievement of the regulatory objectives of consumer protection, market confidence and financial stability. Nevertheless, according to the FSMA 2000, disclosure of confidential information must satisfy at least one of the four conditions addressed in the Act: First, the disclosure must be with regard to the appropriate person, such as the person under investigation or a person who belongs to the same group as the person under investigation; secondly, the confidential information must be information about the person under

[106] *R. v Da Silva* [2007] 1 WLR.
[107] *Ibid.,* p. 308 [E].
[108] *Ibid.,* p. 308 [E and G].
[109] Financial Services and Markets Act 2000, Part XI.
[110] The Financial Services Act 2012 (2012/c. 21), Part 2 (1A).

investigation or one of his group members; thirdly, there must be consent on the part of the person in possession of confidential information which is to be disclosed; and fourthly, the investigators must have the appropriate legal authorization.

The author's view is that the exceptions to the principle of obligatory banking confidentiality are many and varied.[111] Thus, banking confidentiality has become the exception rather than the rule. However, despite the large number of exceptions to the principle of banking confidentiality, the bank is still under a fundamental duty of confidentiality. In that sense, these exceptions do not reduce the importance of banking confidentiality, but rather they try to set limits on the rights of the bank and the customer in its maintenance. Nevertheless, the government must be very careful when making law which authorize the courts to issue any orders for disclosure of a customer's bank information. Jack Committee[112] recommended:

> "The government should not further extend the statutory exceptions to the duty of confidentiality, without taking full account of the consequences for the banker-customer relationship"

The conclusion drawn in this chapter is that disclosure of a customer's private information under compulsory legal provisions has become general rather than exceptional. In this context, the exceptions enable the bank to disclose its customer data at any time by reason of the presence of suspicious activity without it bearing liability for any such disclosure. This could result in the customer losing trust in modern banking practice by reason of the ambiguity in

[111] The Criminal Justice Act 1987, sections 1(3) and 2; the Competition Act 1998, sections 26-27; the Proceeds of Crime Act 2002, part 7 cover money laundering; generally see Griffiths, *op.cit.,* pp. 260-274.
[112] *Report by the Review Committee on Banking Services: Law and Practice*, *op.cit.,* p. 39.

the rules of confidentiality, its scope and its applications. Therefore, there is a need for rules regulating the bank's right to disclose customer's private information. The requirements of these rules are: that they create a programme of control relating to the internet; that they address the issues of staff training, the identification of agents and, of particular importance, the audit; that the principle of verifying customer identity must be included in the banker-customer relationship in order to prove the customer's identity and, if possible, to ascertain whether the customer's transaction involved criminal activities. These rules will allow both the bank and the customer to recognise clearly the circumstances in which the bank has no duty of confidentiality. This view was indeed recommended and observed in the Jack Committee Report. It argued that the principle of confidentiality is deemed to be an essential element in the bank-customer relationship and for that reason that principle should be supported by a regime of codification. Jack's recommendation of regime codification, however, has been rejected, inappropriately in the view of the author, by the UK Government. The government justified this decision with the claim that a regime of codification was needless and likely to create new problems.[113]

[113] *White Paper on Banking Services: Law and Practice* (1990, London, Cm 1026), p. 4.

5.4.2 Disclosure in the public interest

Duty to the public is the second justification for releasing the bank from the duty of confidentiality, and is recognised by Bankes L.J. in *Tournier*.[114] Disclosure under the public interest has been expressed as 'the difficult and comprehensive meaning of the *Tournier* qualification'.[115] These difficulties could be due to a lack of clarity regarding the circumstances which would create exceptions in the public interest. Bankes L.J. in *Tournier* submitted no particular circumstances to define the public interest; he depended on Lord Finlay in *Weld Blundell v Stephens*,[116] when he described the public interest as "danger to the State or public duty may supersede the duty of the agent to his principal."[117] Bankes L.J.[118] submitted, however that the public interest qualification is not fixed; hence it could change from time to time. He presented examples of what could be public interest: in time of war a bank may be forced to disclose to the government information which it receives about the customer's dealings with an enemy alien. His Lordship further held that the application of the exception might be subject to variations at different periods.[119]

Generally, there is no particular standard for what could be constituted a public interest. Griffiths[120] agrees that the qualification of public interest is still not

[114] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461at p. 473.
[115] Hapgood, et al., *op.cit*., p. 159.
[116] *Weld Blundell v Stephens* [1920] A.C. 956.
[117] *Ibid.*, at pp. 965-966.
[118] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461.at p. 479.
[119] *Ibid*., at p. 480.
[120] Griffiths, *op.cit*., p. 277.

completely clear. This qualification has been rejected by Jack Committee Report:[121]

> "Some light may be shed on what in modern conditions, are the public interest considerations likely to justify a bank in departing from the obligations of confidentiality, by reference to the circumstances in which a journalist can be required to disclose his "sources" under the Contempt of Court Act 1980. There circumstances are that the disclosure is "necessary in the interests of justice or national security or the prevention of disorder or crime"... We therefore conclude that banks should no longer be released from their confidentiality obligation on the generalised ground of public interest."

Jack recommended that such exceptions have to be deleted,[122] because it is difficult to formulate a definition of the public interest.[123] The government however has rejected any such suggestion.[124] Effectively there are not many cases where the courts allow disclosure under this exception. *Libyan Arab Foreign Bank v Bankers Trust Co,*[125] which constituted the order for freezing Libyan assets, fell within the qualification of public interest. Staughton J. held:

> "But presuming as I must that New York law on this point is the same as English law, it seems to me that the Federal Reserve Board, as the central banking system in the United States, may have a public duty to perform in obtaining information from banks. I accept the argument that higher public duty is one of the exceptions to a banker's duty of confidence and I am prepared to reach a tentative conclusion that the exception applied in this case."[126]

The author's view is that, for a breach of the bank's duty of confidentiality to accord with the public interest, it has to be specified and not subsumed under a general definition. It is reasonable for the government to identify exactly the circumstances and conditions by obtaining an order from the court which

[121] *Report by the Review Committee on Banking Services: Law and Practice, op.cit.*, p. 35.
[122] *Ibid.,* at p. 37.
[123] *Ibid*., at p. 35.
[124] *White Paper on Banking Services: Law and Practice, op. cit.,* p. 15.
[125] *Libyan Arab Foreign Bank v Bankers Trust Co* [1989] Q.B. 728.
[126] *Ibid.,* at p. 771.

requires the bank to reveal its customers' information under this exception. But since the court already has, under a number of statutes and regulations, the right to order the bank to disclose its customers' confidential information, then it is in fact reasonable to consider this qualification redundant.

5.4.3 Disclosure in the bank's own interest

The bank's own interest is considered to be the third exception to the bank's duty of confidentiality as identified by Bankes L.J.[127] The best case for this exception is when a legal dispute arises between the bank and the customer in relation to the customer's bank accounts, for example repayment of overdraft.[128] Here the bank must evidence the amount of the overdraft on a summons which is a public document.[129] At first sight, this disclosure in defence of bank interests is sanctioned, whereas as a matter of law, certainly this disclosure falls within the public interest for the purpose of the effective administration of justice.[130]

In *Sunderland v Barclays Bank Limited,*[131] the bank did not pay a cheque drawn on it by one of its customers because the funds in the account were inadequate to cover the cheque. The customer called the bank to explain the reason behind non-payment of the cheque, and then she had handed the telephone to her husband who took over the conversation with the bank which she had begun.[132] The manager of the bank informed the husband the cheques were drawn in

[127] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B at p. 473.
[128] Ibid., at p. 473 per Bankes L.J., and p. 481 per Scrutton L.J.; Further, see Charles, *op. cit.,* p. 693.
[129] Alhosani, *op. cit.,* p. 14.
[130] Ross, *op. cit*., p. 175.
[131] *Sunderland v Barclays Bank Limited* (1938) 5 LDAB 163.
[132] *Ibid.*

payment of gambling debts.[133] The customer sued the bank because she thought that the bank breached its duty of confidentiality to her by disclosing confidential information. Du Parcq, L.J. held that there was no breach of confidentiality, because the bank acted to protect its interest and also the plaintiff had given her implicit approval to waive her right to confidentiality.[134]

In *Sunderland v Barclays Bank Limited*, however, the appropriate explanation of the bank's right to disclose its customer information was that in order to maintain its reputation, nevertheless there was no reasonable justification for the bank's action in informing the plaintiff's husband that the cheque was drawn as a result of gambling debts It would have been sufficient to let the husband know that the bank did not guarantee the cheques because there was inadequate money in his wife's account.[135] Alhosani believes that the bank's action could be justified, if either it was the husband's liability to pay his wife's debts or if they had a joint account in the same bank.[136]

It seems that this exception was not generally accepted and prefers to keep the ambit of this exception within fairly narrow confine. Furthermore, this exception accepts when it related to the public interest and not to the bank's interest alone, since allowing such a qualification gives the bank a potential for abuse.[137] In this regard, the Jack Committee clarified significant two subjects of concern.[138] First, the bank considers favourably references from other entities of the same banking group. So there is concern about the exchanging of

[133] *Ibid.*
[134] *Ibid.*
[135] Ellinger, et al., *op.cit*., p.192.
[136] Alhosani, *op. cit.,* p. 15.
[137] Cranston, *op.cit.,* pp.174-176.
[138] *Report by the Review Committee on Banking Services: Law and Practice, op.cit.*, p.35.

confidential customer data between different entities of the same banking group.[139] It is obvious that the bank has no right to exchange and share its customer's confidential information between different members of the same banking group, and any such revelation would place the bank under liability for breach of its duty of confidentiality,[140] that is because each member of a banking group has a separate corporate personality,[141] nevertheless, there is concern that banks might justify all such disclosures as being in their interests. In contrast, the Jack Committee recommended that disclosures of confidential information within the same banking group should be acceptable even in the absence of customer approval.[142] It also recommended that such disclosure should be accompanied by significant awareness of the particular aim of guarding the bank and the damages that it might suffer in presenting standard banking services. However, the bank is considered in breach of its duty of confidentiality if it exchanges and shares customer information for marketing purposes.[143]The authors' view is that such a provision might open the gates to the banks disclosing its customer information for any reason other than marketing and claiming that, since the disclosure was not for the purpose of marketing, there was no breach of confidentiality.

The Lending Code 2012[144] clarifies that, for marketing purposes, the bank must obtain the customer's specific consent before providing the customer's information to any firm, whether in the same group or not. Accordingly, most

[139] *Ibid.*, for the second concern see section 5.5.
[140] Ellinger, et al., *op.cit*., p.192.
[141] *Bank of Tokyo Ltd v Karoon* [1987] A.C. 45 at pp. 53-54; *Bhogal v Punjab National Bank* [1988] 2 All E.R. 296 at p. 305.
[142] *Report by the Review Committee on Banking Services: Law and Practice, op.cit.*, p.35.
[143] *Ibid.*
[144] Lending Code 2012, section 2[23] http://boini.bankofireland.com/fs/doc/wysiwyg/lendingcode.pdf 5 March 2013.

bankers started to protect themselves by including in their contracts with customers a term stating that the bank has the right to exchange and share customer information with other banks in the same group, irrespective of whether that exchange takes place in the UK or overseas.[145] Furthermore, some banks have standard terms and conditions in their contracts which include the provision that they may share and exchange customer information with a third party who is outside the banking group.[146] Normally and in practice, these standard terms and conditions justify disclosure in the banks' own interest, and the customer has no right to discuss such terms because they are considered as a standard in the contract.

In the final analysis, the author's view is that as long as the bank is subject to the management and control of the banking group, directly or indirectly, it is difficult to withhold the transmission of confidential information related to customers dealing with that bank. The holding company is in charge of setting general policy for the activities of its subsidiaries in various fields, based on information received from its subsidiaries. Therefore, it is acceptable to exchange and share customer information within the same banking group. The author believes that if this qualification is given comprehensive interpretation; it could include the bank's commercial convenience and utility, where the bank can justify any disclosure in its own interest. Thus, disclosure in the public interest serves as the best justification for disclosing confidential information.[147]

[145] HSBC, *General Terms and Conditions, op.cit.,* [34.3]; Barclays, *Barclays Terms:* Your *Agreement with Us, op.cit.,* section G[2]; Lloyds TSB, *Personal Banking terms and conditions, op.cit.,* section D[14.1].
[146] Lloyds TSB, *Personal Banking terms and conditions, op.cit.,* section D[14.10].
[147] Alhosani, *op. cit*., 1 at p.16.

5.4.4 Disclosure under the customer's authority

The customer's consent is considered to be the fourth qualification in *Tournier.*[148] The customer's approval could be either explicit or implicit.[149] A customer can permit the transfer of particular items of his personal information. The bank must disclose only the information for which the customer has given explicit approval and no more.[150] It is difficult to indicate exactly the point where the bank obtains implicit approval. In *Tournier,* the court held that the best instance of a customer's implicit approval for the revelation of confidential information is when that customer authorizes the bank to provide a reference.[151] This approach has been adopted by the banking sector for years.[152] However, it is sensible not to assume that a customer who provides his bank details when applying for a credit card is giving implicit approval for the disclosure of confidential information by the bank. *Tournier* has therefore been exposed to criticism in this respect.[153] One of the Jack Committee suggestions was that at the beginning of the bank-customer relationship the bank should explain and describe very clearly how the banking system works and should invite customers to give or withhold a general approval for their banks to submit opinions on them in response to government enquiries.[154] Nevertheless, there is nothing to prevent a bank from including in its contract with the customer a term

[148] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B at p.473.
[149] *Ibid.*
[150] Lending Code 2012, section 2[24].
[151] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B at p. 473 per Bankes L.J. and p. 486 per Atkin L.J.
[152] *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] A.C. 465 at p. 503 and p. 540.
[153] Hapgood, M., *Paget's Law of Banking* (1996), p. 124, not motioned in the 2007, 13th Edition; Chorley, L., *Law of Banking* (1974), p. 24.
[154] *Report by the Review Committee on Banking Services: Law and Practice, op.cit.*, p. 48.

authorizing disclosure of information on a customer's creditworthiness. Furthermore, the Lending Code, 2012 stipulates that the bank can pass negative information without the customer's approval,[155] although the customer must be given notice that the negative information will be passed at least 28 days before the disclosure is made. Within this period, the customer must be given notice, and the ways in which the negative information may affect his ability to obtain credit must be explained.[156] This clarification notice will give the customer a period of time (28 days) during which there will be the opportunity to make repayment or to reach some other settlement arrangement with the bank to enable him to try to replay or come to some arrangement with the bank before negative information is passed to the third party.[157] Before providing positive information in a reference the bank must obtain the customer's approval.[158] Nevertheless, the Code 2012 came without any indication of the type of prior approval required before the passing of positive information, whether explicit or implicit.

In *Turner v Royal Bank of Scotland Plc,*[159] the defendant bank responded in unfavourable terms to a number of status enquiries from another bank about the creditworthiness of the claimant, who held both personal and business accounts with the defendant. The defendant used confidential information concerning the state of the claimant's account when formulating its response. According to the banking practice in that time, the defendant bank did not obtain the customer's express approval before responding to the status enquiries. The customer sued

[155] The Lending Code 2012, section 3[40].
[156] *Ibid.*, at section 3[41].
[157] *Ibid.*
[158] *Ibid.*, at section 3[48].
[159] *Turner v Royal Bank of Scotland Plc* [2001] EWCA CIV 64.

the bank for breached its duty of confidentiality. The Court of Appeal[160] however, held that a bank could not depend on banking practice to justify the assumption of its customer's implied approval for the use of private details in providing other banks with references. Therefore, the theory that the bank could pass on its customer's confidential information on the grounds that the bank has its customer's implied consent is rejected. Hooley argues that *Turner's* decision presents a clear explanation in the area of implied consent theory.[161]

There are, however, double limitations upon the scope of *Turner*. First of all, *Turner* presents no final norms to determine whether a bank can depend on its customer's general approval in responding to status enquiries, or whether the customer's particular approval is required. Ellinger, et al. agree that a bank can depend on its customer's general approval in responding to status enquiries,[162] but the consequence of allowing a bank to depend on a customer's general approval must be that the bank bears the burden of confirming that the customer is informed of the way in which the bankers' reference scheme operates.[163] Secondly, *Turner* surely expands a customer's right to establish liability against a bank for breaching its duty of confidentiality by reporting customer private data to a third party with the absence of a customer's approval, albeit the customer may find difficulty in recovering consequential damages as a result of that breach.[164] Despite the fact that general damages will usually be available,[165] particular damages are not always easy to recover.

---

[160] *Ibid.*
[161] Hooley, R., 'Bankers' references and the bank's duty of confidentiality: when practice does not make perfect', (2000) 59 *The Cambridge Law Journal* 21 at p. 22.
[162] Ellinger, et al., *op.cit.,* at p. 196.
[163] Hooley, *op. cit.,* p. 23.
[164] Ellinger, et al., *op.cit.,* p. 197.
[165] *Turner v Royal Bank of Scotland Plc* [2001] EWCA CIV 64 at [40].

If the bank reveals accurate data that is positive to the customer it is improbable that the customer will to suffer any adverse consequences resulting in loss. Nevertheless this is not an absolute norm:[166] if the data is accurate, but negative, it would be difficult for the customer to prove that the disclosures without his approval caused such losses.[167] The only case where particular damages would probably be easily recoverable is where the data provided by the bank proves to be inaccurate. In such a case, the customer will also have a concurrent claim based upon the breach of the bank's duty of skill and care.[168] In this regard, it is the author's strong recommendation that the principles governing the bank's duty of confidentiality should be regulated by statute in order to avoid ambiguities.

Given the above position, it seems that the law has been changed and thus *Sunderland* is no longer suitable to apply. Therefore, the Court of Appeal in *Turner* held that the bank has no right to disclose or exchange customer's confidential information depending on customer's implied consent. In *Sunderland,* however, the court held that the bank can rely on implied authority and further, that the marriage relationship is significant. Thus, when the wife authorized her husband to call the bank, the court assumed that the claimant gave her implied authority to discuss all related issues.[169] Although, implied consent may exist in particular cases, its scope is very limited. Therefore, banks need to be extremely careful when relying on implied consent as a basis for disclosing customer information.

---

[166] *Jackson v Royal Bank of Scotland* [2005] 1 W.L.R. 377.
[167] *Turner v Royal Bank of Scotland Plc* [2001] EWCA CIV 64 at [39].
[168] Toulson, R. G. and Phipps, C. M, *Confidentiality* (2006), paras. [3-092]-[3-097]; Further, see chapter six.
[169] *Sunderland v Barclays Bank Limited* (1938) 5 LDAB 163.

In this regard, the author's view is that the bank has to notify its customer about any reference before it is transmitted. Moreover, the bank is required to obtain the customer's written consent before any action is taken with regard to the reference. However, a distinction is made between personal accounts and business accounts. Thus, some legal authors' hold that such principles apply only to personal accounts and not to business accounts.[170] Overall, it is fair practice to obtain the customer's express consent before passing any confidential information to another bank and if it fails to do so it will be liable for breach of a duty of confidentiality. Moreover, unless there is a legal reason the bank has no right to refuse to disclose customer's information if such disclosure is in accordance with the customer's request. In practice, the bank could give advice to the customer, explaining that the bank could not act on the customer's request as long as there are good reasons for not so acting.

[170] Hooley, *op.cit.,* pp. 21-22.

5.5 Disclosure of customer credit data to the Credit Reference Agencies (CRAs): legal issues

The development of banking and in particular the growth of EFT makes it possible for banks to execute increasingly sophisticated analyses of their customers' saving and spending habits, which enable banks to market their own products more effectively and also provide a potentially very valuable source of marketing information and facts for third parties, including other financial institutions, retailers, and the CRAs.[171] Disclosure of customer credit data to the CRAs is the second concern was recognized by the Jack Committee[172] and one of the significant issues which needs highlighting is the ambiguity surrounding the disclosure and exchange of customer data with the CRAs and whether these disclosures and exchanges fall within one of *Tournier* qualification.[173] CRAs are self-governing institutions which obtain and collect various financial data about both customers and businesses.[174] They collect and issue records of individuals' financial affairs.[175] There is no doubt that disclosure of customers'

[171] In the UK there are three main consumer CRAs; Callcredit, Equifax, and Experian
[172] For the first concern see pp.251-252; *Report by the Review Committee on Banking Services: Law and Practice, op.cit.*, p. 35.
[173] Wadsley, J. and Penn, G., *The Law Relating to Domestic Banking* (2000), pp. 137-199; Ferretti, F., *The Law and Consumer Credit Information in the European Community* (2008), p. 96; *Report by the Review Committee on Banking Services: Law and Practice, op.cit.*, pp. 36-37.
[174] Ferretti, F., 'Re-thinking the regulatory environment of credit reporting: could legislation stem privacy and discrimination concerns?', (2006) 14 *Journal of Financial Regulation and Compliance* 254 at p. 255.
[175] CCA 1974 section 145(8) defines a CRAS as: "a person carrying on a business comprising the furnishing of person with information relevant to the financial standing of individuals, being information collected by the agency for that purpose.".

private data to the CRAs is not mandatory or obligatory and that it occurs on a voluntary basis.[176]

No attention has been given to the following issues: first, analysis and determination of the actual function of the CRAs and whether they serve a public purpose for the benefit of users and the sector, or whether they merely supply services in the interest of the banks; second, analysis and determination of whether CRA's falls under The Data Protection Act (DPA) 1998 and whether any defaults should be considered as a breach of statutory duty under the Act. Finally, there is a significant need to analyse and determine whether or not CRAs owe a duty to act with reasonable care and skill regarding the customers' confidential data.

There needs to be an examination, based on the results of the first analysis, of the actual function of the CRAs in order to discover whether they are implements of the public interest or whether they merely supply services in the interest of the banks, and; also whether proposals for UK regimes apply to all the different subjects that consumer credit recording entails. A connected argument is that data credit exchanges through CRA's are executed in the interest of the parties involved. Assuming the validity of CRA services, introducing worthwhile business would indeed be in a party's interest. However, the best argument is that if the CRAs evolved procedures similar to those of the private sector institutions such as banks, an evaluation of the right compliance of consumer credit recording with the necessities of data protection should result in better regulation. If CRA services worked in a manner similar to that of

[176] Ferretti, F., 'Consumer credit information system: a critical review of the literature too little attention paid by lawyers?' (2007) 23 *European Journal of Law and* Economics 71 at p.72.

government institutions and under the government umbrella then they would implement a public interest. Nevertheless, there is no similarity between an action which has community interest and an action which one has an obligation to execute.[177] Thus, it seems that CRA's do not execute a public interest. Furthermore, the bank cannot claim that it is in the public interest to disclose private customer information to the CRA's, because disclosure in the public interest refers only to matters involving the safety of the state or the prevention of criminal activity.[178] It is important to assess the functions of CRA's in order to measure whether the existing law sufficiently defends against one interest prevailing over the other; or at least, there should be an attempt to find a balance between the interests of the parties involved. In this regard, the banks have no right to disclose information to the CRAs on the basis of their own interest. This then leaves the banks dependent on the customer's explicit or implicit approval. The White Paper on Banking Services allows the bank to exchange its customer's negative credit data, such as those involving bankruptcy, without customer's approval, on the grounds of the bank's interests. Positive credit data, however, cannot be thus exchanged. The customer's express approval is required to pass positive information and any information which is to be used for marketing purposes.[179] There is no reasonable justification for making a distinction between positive and negative customer data. The author concurs with the view that the customer's credit data, whether negative or positive, should be treated equally and thus this distinction between

[177] Howells, G., 'Data protection, confidentiality, unfair contract terms, consumer protection and credit references agencies', (1995) *Journal of Business Law* 343 at p. 349.
[178] *Ibid.*
[179] *White Paper on Banking Services: Law and Practice*, *op.cit.,* pp. 15-16; The Lending Code 2012. Nevertheless, the Code 2012 came free from explain the nature of approval to pass positive information whether it is required express or implicit approval.

the two types of data is a flaw in banking practice.[180] Another flaw is that it opens the gate to the bank disclosing its customer information without the customer's approval for any reason other than its use for marketing purposes. A final flaw is the development of electronic data stores and EFT services with an absence of any regulations for exchanging, sharing and controlling new commercial markets or private sector agencies. This leaves customers with no protections and they may discover, for example, that the data provided to the CRAs are under the banks' regulation and control and otherwise unprotected. Therefore, there is a need for particular legal rules intervention to strike a balance between privacy rights, discrimination concerns, and the need of the credit industry.[181]

In practice, most banks have a right to pass and exchange their customers' confidential financial data by giving facts on them terms of their capacity to enter into and fulfil a specific financial commitment.[182] These disclosures and exchanges fall completely under the general terms and conditions of the banker-customer contract and are subject to the customer's general approval. However, these general terms and conditions of the customer contract leave the customer without any real option to accept or reject exchange and disclosures of his data, because rejection by the customer of those terms and conditions will cause the banks to refuse to open an account with that person. It would be salutary to bring the sophisticated electronic technology involved in personal data exchange into the ambit of a data protection regime. As a consequence

[180] Howells, *op.cit.,* p. 350.
[181] Ferretti, Re-thinking the regulatory environment of credit reporting: could legislation stem privacy and discrimination concerns?', *op.cit.,* at p. 254.
[182] For example, see HSBC, *General Terms and Conditions, op.cit.,* [34]; Barclays, *Barclays Terms:* Your *Agreement with Us 2013*, *op.cit.,* section G; Lloyds TSB, *Personal Banking terms and conditions, October 2012*, *op.cit.,* section D[14].

the customer data subject to transfer would not be available to the public and transfers would be made using secure encryption. In the final analysis, it seems that CRA's are private organisations working under government regulations.[183] In conclusion, with regard to CRA's as 'private organisations' it is clear that the existing law is insufficient to protect customers against disclosure of private information and against the interests of the CRA's. Consequently the law needs to find a balance between the interests of the customer and the interests of the organisation involved.

The second issue of whether CRAs fall under DPA 1998[184] is based on an analysis of the CRA system. Data collected and recorded via electronic means falls under the DPA 1998.[185] Nevertheless, according to the Act, collecting and storing electronic data is not processing, unless the data are first registered with a 'data controller'.[186] So as long as the customers' data are stored and exchanged by electronic methods within the CRAs, then they are considered 'controlled' data' and fall under the DPA requirements.[187] If a CRA is regarded as a 'data controller' it will owe a statutory duty to apply and comply with the DPA in relation to all credit data which it controls, and any defaults would be considered a breach of statutory duty under the Act.[188] Consequently, any contravention of any of the requirements of the Act from the CRAs which

[183] CCA 1974; The Consumer Credit (Disclosure of Information) Regulations 2010 (2010/1013); Consumer Credit Regulations 2010 (2010/1010) which replaced UE Consumer Credit Directive 2008 (2008/48/EC).
[184] *R v Brown* [1996] 1 All E.R. 545 HL at p.555.
[185] See section 5.6.1 of this chapter.
[186] Section 17(1) of the DPA 1998; Schedule 1, Part 1 (1) of the Act is defined data controller ''a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed'' and defined ''data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller''.
[187] *Keith Smeaton v Equifax Plc* [2012] EWHC 2322 at para. 2 per Anthony Thornton QC; DPA 1998, Part 2, section 9.
[188] *Keith Smeaton v Equifax Plc* [2012] EWHC 2322.

causes damage or losses to the customer entitles the latter to demand compensation.[189] This provides the customer with a kind of protection, although the CRA has the right to attempt to prove that it took all reasonable care and took all the necessary steps to protect the customer data.

The third and final issue is whether the CRA owes a duty of skill and care to consumers under common law principles. Certainly there is no contractual relationship between the CRA and the customer, and thus there is no contractual liability.

Since there is no contract liability between the CRA and the customer, can there then be an assumption of liability according to a duty of care in tort at common law? In *Customs and Excise Commissioners v Barclays Bank Plc*,[190] the Customs and Excise Commissioners, in seeking to recover outstanding VAT from two companies, gained freezing injunctions for all their assets. Barclays were informed of the injunctions, but later passed payments from the accounts in breach of the injunctions. The Commissioners alleged damages for negligence against Barclays. The court held that Barclays owed no duty of care to the Commissioners, but the House of Lords turnover the decision and held that a duty of care is owed in tort liability for economic damage.[191] The House of Lords held that there was a sufficiently proximate relationship between the bank and the commissioners. The parties' relationship, brought into existence by the orders, was closely proximate and akin to a contract. The bank knew or ought to have known that the commissioners were relying directly on it to protect their

[189] *ibid.*
[190] *Customs and Excise Commissioners v Barclays Bank Plc* [2007] 1 A.C. 181.
[191] *Ibid.,* at p. 184.

interests and in return the bank was entitled to charge the commissioners the reasonable costs of its compliance with the orders.[192] Thus, Barclays was liable for breached its duty of care. The court held that there are three tests for the imposition of a duty of care, viz: the 'assumption of responsibility' test; the 'threefold test'; and the 'incremental' test.

> "Three tests have been used in considering whether a duty of care is owed in tort by a defendant for pure economic loss. The first is whether, objectively, the defendant assumed responsibility for his words or conduct vis-a-vis the claimant, or is to be treated as having done so. The second, the threefold test, requires the claimant to show that the loss was reasonably foreseeable, that there was a relationship with the defendant of sufficient proximity and that imposition of a duty would in all the circumstances be fair, just and reasonable. The third is the incremental test. That test, that new categories of negligence should be developed incrementally and by analogy with established categories, is of limited assistance since it does not provide any qualitative criteria by which to measure whether a duty should be held to arise."[193]

Regarding the CRA, the issue is whether it assumed a responsibility to the customers. Hypothetically, no connection exists between the CRA and the customer, thus it is reasonable not to assume the existence of liability under tort. This point is held by the Court of Appeal in *Keith Smeaton v Equifax Plc.*[194] the court states:

> "It would not be fair, just or reasonable to impose such a duty [duty of care in tort].[195] The judge had erred in concluding that a CRA assumed a responsibility to every member of the public simply by choosing to operate that type of business. Imposing a duty owed to members of the public generally would potentially give rise to an indeterminate liability to an indeterminate class. A co-extensive duty of care in tort would also be otiose, given that the Act provided a detailed code for determining the civil

[192] *Ibid.*, at p.188.
[193] *Ibid.*
[194] *Keith Smeaton v Equifax Plc* [2013] EWCA Civ 108.
[195] Words between square brackets is added.

> liability of credit reference agencies and other data controllers arising out of the improper processing of data"[196]

Thus, CRA's owed no duty to exercise care in tort, although, as 'data controllers' they owed customers civil liability under the DPA 1998, such liability issuing when there was found to be improper processing of data.

In conclusion, the rules stated in *Tournier* are generally accepted and applied in the UK courts. Spearman argues that the limitation principles stated in *Tournier* are not obvious, thus, there is nothing to prevent the application of these principles and their interpretation in a wider context of substantive law, for example, the law of confidence, the misuse of private information and data protection.[197] He presents three reasons to justify his view:

> "First, because the general law of confidence, misuse of private information and data protection provides a framework which is not only principled and detailed but also flexible. Second, because this ensures consistency. Third,…, because it would enable the law of banker's confidentiality to keep pace with development in these substantive areas."[198]

However, with the development of EFT systems these rules have become generally less acceptable. Therefore, it seems that *Tournier* is insufficient to cover all issues surrounding bank's duty of confidentiality in the EFT context, and in particular, its qualifications with regard to the public interest are subsumed within the first qualification, disclosure by compulsion of law, and the third qualification only covers a customer's express consent and not a customer's implied consent. Furthermore, with EFT system development and

[196] *Keith Smeaton v Equifax Plc* [2013] EWCA Civ 108.
[197] Spearman, R., 'Disclosure of confidential information: *Tournier* and ''disclosure in the interests of the bank'' reappraised', (2012) February *Journal of International Banking and Financial Law* 78 at p.78.
[198] *Ibid.*

the great number of different users it is important to add new qualification applying to the circumstance where the customer defaults to protect his data and causes disclosure, whether of his own data or those of other users. Thus, there is a need to establish clear and predictable rules applicable to the law of confidence.[199]

5.6 Analysis of the existing legal rules relating to the bank's duty of confidentiality in the EFT context

In the UK here is no particular regime dealing with the bank's duty of confidentiality. DPA 1998, and the Human Rights Act (HRA) 1998, are considered as the main significant legislations dealing with such duty.

5.6.1 The DPA 1998 and the protection of customers' electronic data

The DPA 1998 deals with electronic data and data internet records.[200] It provides the right to the protection of personal information while taking into account the right to process and transfer an individual's data. Regarding EFT systems dealing with customer data recorded electronically, such data must be classified as 'personal data' to be protected by the DPA 1998. *In Tournier,* the

[199] This thesis proposes model rules for EFT confidential law, see chapter seven, section 7.4.
[200] The DPA 1998, Section 1(1) defines data as information which "(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.".

court held that all customer information delivered to a bank, regardless of the sources of the information, falls under the bank's duty of confidentiality.[201] However, not all customer information recorded electronically is protected under judiciary authority by the DPA 1998. This point was illustrated in *Durant v Financial Services Authority,*[202] where the court held that the meaning of 'personal data' should not be interpreted widely, and does not essentially include all information recorded by a computer. The court recognised that personal data, such as biographical information on the customer recorded by the computer, fall within the DPA 1998. It presented as examples of personal data persons' names, contact telephone number, and home or work address. Auld L.J. held:

> "not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act…"personal data" covered the name of a person or identification of him by some other means, for instance by giving his telephone number or information regarding his working conditions or hobbies."[203]

He also held:

> "The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second is one of focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest."[204]

[201] See section 5.3 above.
[202] *Durant v Financial Services Authority* [2004] F.S.R. 28 at pp. 586-587.
[203] *Ibid.*, at pp. 586-587.
[204] *Ibid.*, at p. 587.

Personal data could be identified as information containing an expressed opinion about the customer's personality.[205] Thereby, banking statistics fall outside the personal data concept even if such statistics originally result from personal data.[206] This is because banking statistics include no personal information referring to the customer's data.

Recording and storing the bank's electronic information is not processing unless it is first registered with a 'data controller',[207] a data controller, being defined for the purposes of this thesis as a bank.[208] The 1998 Act imposes an obligation on a 'data controller' to comply with the 'data protection principles' set out in Part 1, Schedule 1(4). These rules require personal information to be used: fairly and legally; for precisely the aims for which it was collected without any changes, to be sufficient. It should also be relevant and precise, and where important, kept updated. Furthermore, suitable procedures must be taken with regard to unauthorized or illegal use of information and for any damage or losses. Therefore, in the EFT system the bank is considered in breach of its duty of confidentiality if the customer's electronic information is not treated and processed fairly. The bank has to satisfy a minimum of conditions under the Act 1998.[209] *Inter alia*, these conditions are: that the customer approves of the

---

[205] *Ezsias v Welsh Ministers* [2007] All E.R. (D) 65 (Dec) at [59-66], [72], [75], [80], [88], and [104].

[206] *Common Services Agency v Scottish Information Commissioner* [2008] 1 W.L.R. 1550 at p.1560, 1574 and 1576; Further, data in a document can be scanned into a computer programme is inadequate to consider data, see *Smith v Lloyds TSB Bank Plc* [2005] EWHC 246 (Ch).

[207] Section 17(1) of the DPA 1998; Schedule 1, Part 1 (1) of the Act is defined data controller ''a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed'' and defined ''data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller''.

[208] CRAs identified as 'data controllers' with this chapter.

[209] The DPA 1998, schedule 2.

processing of his data; that the data processing is important for the performance or initiation of a contract, or to accord with a non-agreement duty, or that the processing is important for the achievement of particular public goals, for example, the administration of justice. Finally, the processing must be 'important for the purposes of legitimate interests pursued by the data controller or by a third party to whom the data is disclosed'.[210] The Act[211] puts forward further conditions that govern the processing of 'sensitive personal data', such as ethnic origin and religious or political orientation. The customer data will be considered processed unlawfully if the bank fails to comply with these conditions. Furthermore, any processing which results in infringements of the rights of privacy will be considered unlawful processing. The DPA 1998, introduces the right to respect for an individual's data.[212] This involves the person's right of access to his data;[213] it inhibits the processing of an individual's data for the goals of marketing;[214] inhibits any processing that may cause losses;[215] imposes a right to reimbursement where losses result from a breach of the Act's rules,[216] and finally, gives a data subject the right to apply to the court to correct any mistake or alterations in the personal data.[217]

[210] *Ibid.*
[211] *Ibid*., schedule 2, para.6(1).
[212] *Ibid.,* section 55.
[213]*Ibid.*, section 7; However, The Act governs information about persons, but not limited firms or limited responsibility of the partnerships.
[214] *Ibid.,* section 11.
[215] *Ibid.*, section 10.
[216] *Ibid.,* section 13.
[217] *Ibid.,* section 14.

5.6.2 The Human Rights Act 1998 and misuse of customer's confidential information

In order to involve the Human Rights Act 1998 in banking confidentiality in an EFT context, it must first be proved that the duty of confidentiality falls under the European Convention on Human rights and Fundamental Freedoms 1950.[218]

Article 8 of the ECHR deals with respect and protection for personal life, with the aim to protect the individual's privacy and to prevent any violation of privacy under any circumstances, unless there is legal provision allowing for a violation. In *Niemietz v Germany*[219] the court held that an individual's private life in Article 8 of the ECHR involved certain aspects of an individual's professional or business life, especially where a confidential relationship exists to protect individual information, provided the information collected and recorded by a bank concerning an individual customer falls under the professional duty of confidentiality. Therefore, the right to a private life and the protection of personal data addressed by article 8 of the ECHR succeeds in involving a bank's duty of confidentiality.[220]

The human rights rules and those actions which could cause misuse of confidential information are satisfactorily summarised by Tugendhat J. in *Goodwin v News Group Newspapers Ltd*.[221] Tugendhat J. established the

[218] The Human Rights Act 1998 incorporates European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (ECHR hereafter).
[219] *Niemietz v Germany* (A/251-B) (1993) 16 E.H.R.R. 97.
[220] There is no difference between personal information and business information; *Imerman v Tchenguiz* [2009] EWHC 2902 at [76].
[221] *Goodwin v News Group Newspapers Ltd* [2011] E.M.L.R. 27.

circumstances in which the action could cause misuse of confidential information as follows:[222]

> "a. The starting point is the Human Rights Act 1998. By s.6 the court (as a public authority) is required to act compatibly with Convention Rights. By s.1 (1) the court is also required to take into account judgments of the European Court of Human Rights ("the Strasbourg court"). That is what Parliament, not the judges, has decided. The Convention rights in question in this case are the rights to freedom of expression of NGN and the right of the general public to receive information, which are protected by art.10 and by the common law, and the right to respect for private life protected by art.8."

Article 8(2) establishes the different conditions that must be applied by the public authorities in order to avoid any misuse of a person's confidential information. Article 8(1) enshrines the principle that any contravention or misuse of a person's privacy is illegal. The bank must apply the conditions enshrined in Article 8(2); otherwise it would be in breach of its legal duty. Overall, any interference with the person's rights that falls within Article 8(2) requirements will be illegal. Nevertheless, Article 8(2) lists exceptions to the principles. These exceptions were interference by a public authority in accordance with the law and as deemed necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country; for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The author's view is that when a bank breaches its duty of confidentiality it should reference clearly to the statutory provision which justified this breach, otherwise it would be liable for a breach of the duty of confidentiality under the HRA. Further, for the present aim of this section it is important to adopt a clear

[222] *Ibid.,* at [62].

approach to avoid any misuse of customer's data. This involves applying Article 8 to a bank's duty of confidentiality in order to protect a customer's data from any unlawful interference unless it is provided by the law. Consequently any use of the power of revelation as, for example, when confidential customer details held by a bank are revealed under common law, must take into account its proportionality to the legal goal pursued. Finally, with the expansion of the general law protecting privacy there is no reason why the HRA 1998 rules should not encompass the banker-customer contract.[223]

Ultimately, EFT transactions deal with information more than with cash transactions. Thus, there are risks from hacking or unauthorized internet data being captured. Therefore, there is a need for more clarity regarding the means by which banks control, save, and employ the customers' information and further there is a necessity to protect and prevent any misuse of the customers' data. The existing law for determining the legal validity and liability for the security procedures in the protection of a customer's electronic data against any unauthorized attack will be discussed in a subsequent section.

5.6.3 The procedures actions against unauthorized access or any attack in the context of EFT

The confidentiality of EFT systems means the banks have to protect EFT transaction information from being accessed by hackers. This protection can be done by encrypting information communication by such means as hiding a

[223] *Wilson v First County Trust Ltd (No 2)* [2004] 1 A.C. 816.

customer's identity through the use of certain techniques.[224] Azzouni addressed two significant problems that could be associated with electronic banking confidentiality.[225] First, the bank has to provide different methods to protect both the customer's confidential information and the bank's encryption. Secondly, with EFT transactions there is a risk of unauthorized attacks on the customers' data.[226] Azzouni believed that these problems could be solved by adopting strict laws sufficient to deter hackers.[227] Thus, it is significant to look at the laws that can be applied to these types of attack.

The first problem is that the banks need to supply sophisticated encryption methods to protect both the customer's confidential information and the bank. Such problems can be solved by adopting a highly secret system to prevent any unauthorized access to the bank's electronic data.[228] Nonetheless, the first step in protecting a customer's information could be through the privacy of the information about each party involved in the EFT transaction. Neither payers nor payees have access to each other's personal transactions, irrespective of which type of EFT method is used, thus ensuring their privacy is protected.[229] However, this is not the best solution because of the potential for such information being disclosed by the parties involved in the transaction.[230] Furthermore, with hidden customer identity techniques there is concern that an EFT transaction may involve criminal activities such as money laundering. In

[224] Sadeghi, A. R. and Schneider, M., 'Electronic Payment Systems', in Becker, E., *Digital Rights Management* (2003), p.117.
[225] Azzouni, A., 'Internet banking and the law: a critical examination of the legal controls over internet banking in the UK and their ability to frame, regulate and secure banking on the net', (2003) 18 *International Banking Law and Regulation* 351 at p. 355.
[226] *Ibid.*
[227] *Ibid.*
[228] See chapter four.
[229] Sadeghi, *op.cit*., p.118.
[230] *Ibid.*

addition, this solution does not address the issues surrounding unauthorized access to the customer's data via hackers.

The banks must take all necessary steps to protect customer's confidential information. Within the DPA 1998, as explained above, a person is authorized to be known by any data controller when personal information is being passed by or on behalf of that data controller. This requirement still does not apply clearly. The banks, however, include within their contract with the customer the information that they have very strict security systems designed to avoid attack from hackers and access to the customer's details. It is important to include within the banker-customer contract the provision that customer data will be used only by a legally constituted authority and that the bank will protect the data by offering very high security requirements.[231] In addition, with an EFT system there are different ways by which the bank could send the customer information, such as email and the postal services. The bank is obliged to obey the customer's request to send confidential information in a secure way, for example by special delivery. Thus, sending the information via email will be considered a breach of the banker-customer contract.[232] The author's view is that these different options necessitate legal regulation in order to maintain a high level of security and to protect customer's data in the EFT system. Azzouni illustrates this point by an example: in July 2000 a number of Barclays' customers obtained access to another customer's account information; therefore Barclays had to lock its website. However, no action was taken against the bank for its default in the provision of the security features required

[231] The DPA 1998 Schedule 1, Part 2 (11).
[232] *Brandeaux Advisers (UK) Ltd v Chadwick* [2010] EWHC 3241.

under the DPA 1998 and its breach of contract with the customers.[233] He argues that under the DPA 1998, the bank would be held liable for such disclosure if any action was taken against Barclays in the courts.[234]

The second problem is the validity of legal prohibitions against unauthorized access to the customer data in the EFT system and the criminalization of such action. A legal analysis of the existing laws may help to address the problem of attacks on electronic customer data by hackers and determine the legal liability. In *R. v Governor of Brixton Prison, Ex p. Levin*[235] some answers may be found. The facts are: in 1994 a United States bank, Citibank, was exposed to unauthorized access to its computer system.

The issue started when the Citibank provided its customers with unlimited online access via telephone from any geographic location. Once such service existed customers had the ability to execute different types of transactions, including credit transfers between accounts. Consequently, funds were transferred from the customer accounts into the offender's accounts and those of his accomplice.[236] Some of the offences are under the criminal law of England and Wales: they are the offences of theft, forgery, false accounting and unauthorized modification of computer material.[237] The case is considered as one which identifies the uncertainty of legal issues surrounding the unauthorized access to computer data. In this case the court held that: first, a

[233] Azzouni, *op.cit.,* p. 355.
[234] *Ibid.*
[235] *R. v Governor of Brixton Prison, Ex p. Levin* [1997] Q.B. 65.
[236] *Ibid.*, at p. 71; Levin (offender) who is a Russian citizen was arrested at Stansted Airport on 3 March 1995 in execution of a warrant under section 1(3) of the Extradition Act 1989 at the request of the US Government and detained to await directions of the Secretary of State for his extradition to face 66 charges including offences of wire fraud and bank fraud and of conspiring to commit such offences.
[237] *Ibid.*

person who gains access to bank computer data in an unauthorized way is considered guilty of a crime under the Computer Misuse Act 1990.[238] Further, section 2(1) of the Computer Misuse Act 1990 clarified that unauthorized access is a crime if it involves the purpose of perpetrating or facilitating a further crime. Therefore any attack against customer data from hackers or any other unauthorized person is considered a crime and incurs criminal liability under section 2(1) of the Computer Misuse Act 1990.[239]

On this ground, a bank or its employee falls within this section in the event that they attempt to access customers' accounts or bank system data without legal authority.[240] Therefore, there is nothing to prevent the application of such rules to any kind of hacker and to the crime of gaining unauthorized access crime to an EFT system. Furthermore, the case held that any action with intent to cause an unauthorized modification to a customer's computer data falls under section 3 of the Computer Misuse Act 1990. Thereby, the court held that 'the introduction of an unauthorized instruction to transfer money from the accounts into other accounts would certainly impair the ability of Citibank and its customer to depend on data records in the computer'.[241] The author's view is that there is no reason to prevent application of the same rules in cases of unauthorized access to, or an attack on, a banking computer system. Secondly, in *R. v Governor of Brixton Prison, Ex p. Levin,* the court held that the action of

[238] Computer Misuse Act 1990, section 1.
[239] *R. v Governor of Brixton Prison, Ex p. Levin* [1997] Q.B. 65 at p.71.
[240] *Director of Public Prosecutions v Bignell* [1998] 1 Cr. App. R. 1; *Regina v Bow Street Metropolitan Stipendiary Magistrate and Another* [2000] 2 A.C. 216.
[241] *R. v Governor of Brixton Prison, Ex p. Levin* [1997] Q.B. 65 at p. 78.

issuing unauthorized instructions on the Citibank computer falls under section 17(1) of the Theft Act 1968.[242]

In accordance with the Theft Act 1968 the court held that the applicant made an entry in a continuous record stored on the computer's disk which was unquestionably incorrect or misleading. The applicant was therefore involved in, and charged with, computer misuse, forgery and falsification of accounts.[243] The author's view is that attacks on bank system data and access to them without legal authority involve criminal liability and there is no legal obstacle to applying the principles of *R. v Governor of Brixton Prison, Ex p. Levin* to such a crime. Nevertheless, the EFT system is still in need of regulation in matters relating to internet banking security attacks and unauthorized access to security data. Azzouni[244] argues this point as follows:

> "It can be concluded that although the existing regulations can be applied to cases involving internet banking, they may still be diversity in the interpretation of these provisions. Therefore, legislations should study the current situation of internet banking technology and the provisions that can be applied and make the vital amendments in order to respond to the challenges that may be faced."[245]

[242] *Ibid*., at p. 80.
[243] *Ibid.*
[244] Azzouni, *op.cit*., p.357.
[245] *Ibid.*

5.7 Liability for breach of the duty of confidentiality in an EFT context

A bank's duty of confidentiality could be breached under three main risks: first, the bank discloses its customer's private information without legal authority; secondly, through default of the bank in providing the required security procedures; and thirdly, through unauthorized attack from hackers or an attack without legal authority.[246] This section will be devoted to determining which party bears the losses and damages resulting from the breaches of banking confidentiality. There is an absence of legal regulation covering the liability for breach of banking confidentiality in the EFT system. This absence has led banks to establish their own contractual agreements, terms and conditions. Within these agreements banks are free to use customer data in a comprehensive way, without allowing the customer the right to reject the use of that data.

In regard to the first risk, a bank is in breach of its duty of confidentiality if it discloses the private information without legal authority. Such a breach establishes the bank's liability for any losses and damage suffered by the customer. Nevertheless, if the bank proves that the disclosure was due to the customer's negligence the bank bears no liability towards the customer.

In regard to the second risk, which is default on the part of the bank in providing security procedures, regulation 120(1) of the PSR 2009 provides that any breach of the requirement of Parts 5 and 6 gives the customer the right to claim

[246] For this liability see chapter four.

for loss and damages ensuing from a breach of statutory duty. Regulation 58(1)(a) imposes on the bank a duty to ensure that the personalised security features of the payment instrument are not accessible to persons other than the rightful holder. Thus, this provision could be applied in a case of a default on the part of the bank in providing its computer system with the security requirements necessary to prevent unauthorized access. It is relevant to note here that the banks have the power to control the EFT system[247] and therefore in the case of any breach of the bank's confidentiality, for example, through an attack on the bank security system, the bank bears the loss and damage resulting from such breach. In contrast, with internet banking the banks cannot control the transactions because both the bank and its customers are users of online transactions and therefore the technical malfunctions of the system are outside the control of the bank.[248] Consequently, Lloyds[249] and HSBC[250] for example, have considered the bank not liable for any default or losses due to the technical malfunctions of any internet systems beyond their control. However, the author's view is that exempting the bank from liability due to the technical malfunctions of the online system is not justified unless the banks have presented all the security procedures necessary to prevent the defaults or losses.

Overall, it seems that the bank is liable to the customer for any losses or damage resulting from disclosure of confidential information or data without legal provision or qualifications outside of the law. The bank's liability extends to

[247] Reed, C., *Internet Law*: *Text and Materials* (2004), p. 29.
[248] *Ibid.*
[249] Lloyds TSB, *Terms and conditions* [12.5] http://www.lloyds.com/Common/Help/Terms-and-conditions 20 April 2013.
[250] HSBC, *Terms and Conditions* [9.1] http://www.businessgrant.hsbc.co.uk/terms 20 April 2013.

any economic loss, further it could extent to any suffering of injury in feeling.[251] In another words, the bank should be liable to the customer to recover direct and indirect damages.[252] The bank is liable, also for any disclosure resulting from the default of the bank to provide the required security procedures necessary for the prevention of any unauthorized access to the customer's data. Also, the bank is liable for any disclosure resulting from its employees; such liability arises even if the employees of the bank were negligent. However, there is no liability on the bank if such disclosure was due to the customer's negligence.

5.8 Conclusion

The EFT system should provide as a minimum the same level of confidentiality as cash payment systems. The purpose of the duty of confidentiality is that the EFT system information should not be easily accessible for the purpose of gaining more detailed or broader data about customers. Hence, in the EFT system, a bank's duty of confidentiality can be assessed according to which data they disclose to a particular customer. EFT confidentiality can be achieved by providing a very high standard of encryption for internet data and ensuring that no one can access such data without authority. However, confidentiality within EFT systems cannot prevent the possible transmission outside an EFT system between involved parties, such as internet data networks; or data may be revealed in subsequent commercial interactions. The author's view is that

[251] See chapter six.
[252] *Ibid.*

the existing confidentiality laws do not provide customers with an adequate level of protection and safety to be able to control the recording and exchange of data relating to their EFT transactions. Thus there is a need of new legal rules to protect customer's data in the EFT context. Such legal rules would govern all the exceptions and limitations with regard to disclosure of customer information, and would create a balance between the customer's right to privacy and the third party's interest. Furthermore, these rules should emphasise the duty of employers, for example banks and CRAs, to employ encrypting systems sufficient to prevent any unauthorized access to the banks' data.[253]

This chapter concludes that banking confidentiality is not merely a necessary obligation for the bank to safeguard customer information. It is, at the same time, a positive obligation to ensure that the bank takes all necessary measures and steps to maintain the confidentiality of customer information. Therefore, due to the development of electronic banking the banks must take all reasonable care and have security procedures to prevent any attack or unauthorized access to the bank's accounts, transactions and operations, by every electronic means possible. On the whole, banking confidentiality is not confined to protecting the customers' interests: it is also designed to protect the interests of the banks themselves as well as to strengthen confidence in the banking system. Finally, with all the exceptions explained in this chapter, banks face an increasingly complicated task in reconciling and balancing their different obligations with regard to details and information on their customers and their confidentiality. Customers have significant expectations regarding banking

[253] Barker, K., et al., 'Credit card fraud: awareness and prevention', (2008) 15 *Journal of Financial Crime* 398 at pp. 406-407.

confidentiality. Therefore, in future, both the judiciary and the government should not further extend qualifications to the rules regarding the duty of confidentiality without taking into consideration all the consequences for general law of the advanced technology of the electronic banking sector. Also, they have to make reasoned evaluations regarding the misuse of confidential information.

Chapter Six

Recoverability of EFT Transaction Losses

6.1 Introduction

The most common disputes arising from EFT's involve unauthorized transactions, failures or delays in transfers, or a combination of both failures and delays. Damages attributable to these breaches or delays may include losses to the principal amount of the transaction, interest losses and losses resulting from foreign exchange rate fluctuations between the expected and actual time of receipt the funds transferred. Resolution of these disputes requires the determination of which party is liable for the losses.

Damages in the context of EFT are not covered by statute or case law, except the PSR 2009, when applicable, according to which the payer bank is obliged to refund the transaction funds when the bank made the payment in response to an unauthorized instruction.[1] Furthermore, in case of non-execution or defective execution of a payment instruction a bank is liable to its customer for any funds or interest which must be paid by the customer.[2] However, these provisions may be disapplied, when the customer is not a consumer, if there is an agreement between the parties.[3] If one of the EFT parties breaches its contractual duties, such a breach confers a recoverability right on the injured

[1] The PSR 2009, regulation 61.
[2] *Ibid.,* regulation 77.
[3] *Ibid.,* regulation 51(3)(a).

party.[4] Within the basic principles covering actions for breach of contract, the innocent party is authorized to recover damages from the party in breach, but unless the innocent party has sustained a loss, that party is confined to recovering nominal damages.[5] This general rule is applicable where the bank debited their customers' accounts without a customer's mandate or made the transfer incorrectly. The bank has no right to debit its customer account without the customer's mandate; accordingly the customer has the right to request the bank that acted without customer's mandate to re-credit the account instead of following the funds transferred.

This chapter is devoted, first, to examining what kind of damages are recovered in EFT transactions and, second, to determining the party which bears the losses. In modern practice, agreements between a bank and a customer tend to relieve the former from bearing any liability towards the customer, thus making the damage recovery process for customers almost non-existent. The outlines of this chapter are as follows: section 6.2 is devoted to explaining the measure of damages for breach of contractual duties and its applicability to EFT transactions. This section clarifies the notion of damages; it illustrates that the term damages always refers to the money recovered from losses resulting from any breach in the contract. Also, this section demonstrates that the general principles for the measure of damages for breach of contractual duties could be applied to damages for breaches in an EFT transaction. Section 6.3 is devoted to examining the categories of damages which could be classified as direct

[4] Kilonzo, K.D., 'An analysis of the legal challenges posed by electronic banking', (2007) 1 *Kenya Law Review* 323 at p. 325; Robertson, A., 'The basis of the remoteness rule in contract', (2008) 28 *Legal Studies* 172 at p. 172.
[5] Chitty, J. D., *Chitty on Contracts* (2008), para. 26-998.

damage and consequential damage. When the bank acts outside the customer's mandate, the customer loses the principal amount of money, the interest that the payer might have been be paid if that amount of money had been in the account, and possibly that customer may suffer consequential damages, such as the loss of a favourable contract. In practice, the bank is normally liable for direct damage and avoids or limits its liabilities for consequential damages. This section demonstrates that the recoverability of consequential damages in EFT transactions is uncertain, and that uncertainty may give cause for concern in the banking sector. One of the more significant findings to emerge from this chapter is that there is a need for legal rules which allocate risk of direct damages and consequential damages. The chapter then proposes model rules which should be of benefit in regulating the banks' liability for consequential damages.

6.2 The measure of damages for breach of contractual duty and its applicability to EFT transactions

Since the banker-customer relationship is contractual, the payer's bank's accountability for damages can be defined by adopting the general principles of contract law.[6] There is consensus in the literature that damages are a remedial measure in the form of compensation awarded to the innocent party as a result of incurred expenditure or losses, caused by a breach of one of the contract

[6] *Agip (Africa) Ltd v Jackson* [1991] Ch. 547 at p. 549; Kethi, K., 'An Analysis of the Legal Challenges posed by Electronic Banking', (2007) *Kenya Law Review* 323 at p. 334.

duties.[7] The measure of damages under common law rules is demonstrated by Parke B. in *Robinson v Harman*.[8] Parke B. held that any party in the contract who sustains a loss by reason of a breach of contract is entitled to obtain reimbursement and "so far as money can do it, to be placed in the same situation with regard to damages as if the contract had been performed".[9] Thus, the paying bank which acted outside its customer's mandate, for example, by debiting payer's account in accordance with an unauthorized instruction as a consequence triggers the bank's liability for damages to the customer,[10] and that customer should then be returned to the same position he would he have been in had the account not been debited or the payment instruction had in fact been transferred to the required payee.[11] The application of this measure is restricted by the test of remoteness initially formulated by the rule in *Hadley v Baxendale*.[12] Alderson B. held that the damages were awarded for breach of contract either arising naturally or not arising naturally if such losses were within the contemplation of both parties when they signed the contract.[13] In *Hadley v Baxendale* the plaintiff's claim for loss of profit was dismissed because "it is obvious that, in the great multitude of cases of millers sending off broken shafts

[7] Haynes, A., *The Law Relating to International Banking* (2010), pp. 257-258; McKendrick, E., *Contract Law* (2010), p. 757 and pp. 816-817; McGregor, H., *McGregor on Damages* (2009), p. 3; Harris, D., et al., *Remedies in Contract and Tort* (2005), pp. 14-15; Wadsley, J., and Penn, A. G., *The Law Relating to Domestic Banking* (2000), p. 215; Bergsten, E. E., 'Legal aspects of international Electronic Funds Transfers', (1987) 7 *International Business Law* 649 at p. 659.
[8] *Robinson v Harman* (1848) 154 E.R. 363; *Jackson v Royal Bank of Scotland* [2005] 1 W.L.R. 377; further, see Edelman, J., *Gain-Based Damages: Contract, Tort, Equity and Intellectual Property* (2002), p. 22.
[9] *Robinson v Harman* (1848) 154 E.R. 363 at p. 365.
[10] Bergsten, *op. cit.,* pp. 659-660.
[11] Fofaria, A., 'Excluding the recovery of "consequential and indirect losses" in English and French laws', (2006) 5 *International Business Law* 597 at p. 601.
[12] *Hadley v Baxendale* [1854] 9 Ex. 341.
[13] *Ibid.* at p. 354; Also, see Hood, P., 'Remoteness of damage in contract revisited', (1996) *Edinburgh Law Review* 127 at p. 127; Fofaria, *op. cit.,* p. 602; Odry, G., 'Exclusion of consequential damages: write what you mean', (2012) 29 (2) *The International Construction Law Review* 142 at p. 154; Tettenborn, A., 'Consequential damages in contract-the poor relation?', (2008) 42 *Loyola of Los Angeles Law Review* 177 at p. 182.

to third persons by a carrier under ordinary circumstances, such consequences would not, in all probability, have occurred; and these special circumstances were here never communicated by the plaintiffs to the defendants."[14]

Within EFT transactions, since the banker-customer relationships is contractual relationship, the measure of damages is only applicable when the bank breached one of its contractual duties.[15] In this regard, in the absence of a contractual agreement between the bank and the person, bank is under no duty, to this person, to execute an EFT transaction. As such, no damages are recoverable if the bank fails to execute a payment instruction. The banks are under a duty to exercise reasonable care and skill to execute their customers' instructions. Nevertheless if there is no wrongdoing or breach from the bank, there are no recoverable damages.[16] For example, if the paying bank fails to acknowledge the receipt of a payment message so that it is not included in the settlement for the day; the paying bank bears no liability to its customer if it has acted reasonably in attempting to make payment.[17]

6.3 Damage category for recovery of EFT losses

When an EFT instruction is issued or altered fraudulently the payer loses the principal funds, the interest that the customer might have been paid had those funds been in his account, and also perhaps consequential damages, for example, losing a preferable contract. Such damages are direct damages,

[14] *Hadley v Baxendale* [1854] 9 Ex. 341 at p. 356.
[15] *Jackson v Royal Bank of Scotland* [2005] 1 W.L.R. 377 at p. 377.
[16] Arora, A., 'Contractual and tortious liability in EFT transactions in the United Kingdom', (1992) 1 *Law, Computers & Artificial Intelligence* 291 at p. 304.
[17] *Ibid.*

consequential damages and loss of interest. At first view it may seem odd to assert that there is a difference between direct and consequential damage.[18] When a person has breached his contractual duties, that person will be responsible for any damages expected to result from such a breach to the same measure of damage, without increase or decrease.[19] Such damages are considered direct damages. In reality, there is a difference between damages classed as necessary and immediate, and those which are foreseeable and consequential. For foreseeable and consequential damages, the injured person will face more difficulty in proving the damages.[20]

6.3.1 Direct damage

A bank which defaults in executing its customer's EFT instruction does not create direct damages equivalent to the principle amount of the instruction because no funds have been transferred from the customer's account. The customer may nonetheless suffer losses on the service charges payable to another bank for processing such transfers since, owing to the failure to make the payment, the customer may have to make use of another bank's services. He will also stand to incur losses in the difference between service charges if the latter bank applies higher service charges.

Where the bank executed the EFT instruction incorrectly and thus the funds transfer is not completed, a customer may suffer damages. These damages

[18] Tettenborn, *op. cit.,* p.181.
[19] *Ibid.*
[20] *Ibid.* at pp. 181-182.

may include the principal sum of the transaction and loss of the use of such money until the bank refunds the transaction funds to his account or corrects the funds transfer by executing it in conformity with the EFT orders given. Furthermore, except when the funds transfer is corrected, the customer will lose any fees, including the expenses paid, in the funds transfer. Also, in the case of insolvency, the payee may suffer losses as a penalty for late payment or non-payment,[21] and the payee's direct damages will be the interest on the principal amount for the time of delay. However, in practice the payee will possibly sue the payer for such losses. In this case, the principal sum of the transaction or its charges or fees is outside the calculation because there is no loss. These are the direct damages that a customer would typically lose for a bank's failure to carry out an EFT instruction. In banking practice, such failure results from a bank's error or negligence.

Whether such damages are recoverable depends on the measure of damages applicable. It was argued previously that the measure of damages for breach of contract is applicable to the banker-customer contractual agreement in EFT transactions. [22] In *Jackson v Royal Bank of Scotland*[23] the House of Lords considered the damages that should be awarded against a bank for breach of a contractual duty of confidence. The transaction under which that duty arose concerned a transferable letter of credit that had been issued by the defendant bank to the customer in favour of the claimants. In this case, the claimants imported goods from a company in Thailand to sell on to a customer in Lancashire. The customer was aware of the name and contract information of

[21] Ellinger, E., et al., *Modern Banking Law* (2011), p. 509.
[22] *Jackson v Royal Bank of Scotland* [2005] 1 W.L.R. 377 at p. 390.
[23] *Ibid.,* at p. 377.

the Thai provider but was inexperienced in importing goods and relied on the claimants to handle the paperwork, import formalities and delivery of the goods to its premises. At the customer's request, the claimants ordered goods from the Thai provider which the claimants sold on to the customer. The claimants transferred the benefit of some of the credit to the Thai provider as the means by which the claimants would pay the Thai provider. The claimants kept the difference to cover their cost and as their profit. The defendant bank, when handling one of the letters of credit, mistakenly sent to the customer documents which should have been sent to the claimants. One of those documents revealed to the customer the amount of the profit made by the claimants on the transaction. As a result the customer stopped dealing with the claimants and thus, there were no further orders from the customer. Instead he signed a contract directly with the Thai provider. The claimants sued the bank for the lost opportunity to make further profits from the trading relationship with the customer (the consequential damages).[24] The House of Lords held that as the customer knew the Thai provider and could have made investigations of the Thai provider at any time which would have discovered the amount of the claimants' profit, therefore there was no loss suffered by the claimants. One of the issues dealt by the House of Lords in this case is whether the damages that the claimants claimed was too remote to be predictable at the time of the signing the contract, thus it was not recoverable.[25]

Lord Hope held that according to the two rules of *Hadley v Baxendale,* damages are not recoverable except where it has been in the contemplation of

[24] *Ibid*.
[25] *Ibid*., at p.387 per Lord Hope.

both parties at the time they made their contract.[26] Therefore, there was no argument that the bank was aware of any special circumstances and it accepted to bear any special loss which was referable to special circumstances at the time of the signing of the contract.[27] Therefore the losses that the claimants claimed were within the first rule of *Hadley v Baxendale,* because the damages were predictable, at the time of signing of the contract, to arise in the normal course from the bank's breach of contract in revealing the confidential documents to the customer.[28]

Arora[29] confirms that, when the paying bank fails to execute the customer's mandate correctly because of negligence, the measure of damages recoverable by the customer of the paying bank will be similar to the damages recoverable in breach of contract, for example, reimbursement for such loss as is reasonably predictable as a consequence of a breach of the kind in question. The damages recoverable by the customer of the paying bank not only cover the funds of the EFT transaction that should have been made, or the funds of the transaction which was incorrectly made:[30] such reimbursement should also cover any injury caused to the customer.[31] In this regard, the bank's customer should be put, so far as money can do it, in the same place he would have been in, had his payment order been executed as instructed.[32] This should take into account the remoteness rule of *Hadley v Baxendale.* In accordance with the

[26] *Ibid.*
[27] McKnight, A., 'A review of developments in English law during 2005: part 1', (2006) 21 *International Banking Law and Regulation* 117 at p. 139; McMeel, G., 'Contract damages: the interplay of remoteness and loss of a chance' (2004) 1 *Lloyd's Maritime and Commercial Law Quarterly* 10 at p. 13.
[28] *Jackson v Royal Bank of Scotland* [2005] 1 W.L.R. 377 at p. 390 per Lord Hope.
[29] Arora, A., *Electronic Banking and the Law* (1988), p. 72.
[30] *Ibid.*
[31] *Ibid.*
[32] *Robinson v Harman* (1848) 154 E.R. 363 at p. 365.

rules formulated in *Hadley v Baxendale,* it seems that the customer is entitled to recover from his bank the following damages, which could be identified as direct damages 'arising naturally', from the execution of a payment instruction outside of a customer's mandate; and that such damages arise "according to the usual course of things";[33] firstly, the principal amount lost in the transfer; secondly, the expenses and fees the payer paid to the paying bank to make payment to the particular payee;[34] and thirdly, the interest of the principal amount from the day it is debited from the customer's account until the date the paying bank refunds the customer's account.

Under the PSR 2009,[35] when the payer's bank executes a payment instruction that was not authorized by the payer, the payer's bank must immediately refund the amount of the unauthorized payment instruction to the payer. Furthermore, the payer's bank is liable to restore the debited payment account to the state it would have been in had the unauthorized payment transaction not taken place.[36] It seems that the payer's bank is liable to the payer to recover the principal amount of the unauthorized transaction, the interest of the amount debited without authorization and any other fees paid by the payer to make the payment.

[33] *Hadley v Baxendale* [1854] 9 Ex. 341 at p. 354.
[34] *Ibid.,* at p.354 and p. 465; Halladay, M. J., 'Remoteness of contractual damages', (2009) 21 *The Denning Law Journal* 173 at p.174.
[35] PSR 2009, regulation 61(a).
[36] *Ibid.,* regulation 61(b).

6.3.2 Consequential damage

Debiting the customer's account according to an unauthorized transaction may deprive the customer of other opportunities, such as the fund that had been debited from the account to buy shares at low prices, or result in the nullification of an important business contract or a poor credit rating or other damages.[37] According to the second test of *Hadley v Baxendale,* consequential damages are not recoverable except in cases where they were "reasonably to have been in the contemplation of both parties, at the time they made the contract, as the probable result of the breach of it".[38] From this it could be deduced that when the bank is aware of the fact that the failure in funds transfer would lead to losses for the customer, the customer is entitled to recover consequential damages.[39] The common law rules hold that the defendant's liability for consequential damages issues from the defendant's awareness of the special circumstances that caused the claimant's losses.[40] Conversely, if the defendant is not aware of such special circumstances, the customer is not entitled to recover consequential damages.[41] The claim for the recovery of consequential losses will be inadequate unless the customer has shown or proved that the defendant, the bank was aware of the consequential damage.[42] Therefore the bank and the customer must be aware of that damage which might occur as a result of the special conditions, and also it must be within the contemplation of

[37] Ellinger, et al., *op.cit.,* p. 509.
[38] *Hadley v Baxendale* [1854] 9 Ex. 341 at p. 354
[39] *Simpson v London & North Western Railway Co* (1876) 1 Q.B.D. 274; *Seven Seas Properties Ltd v AL-Essa (No.2)* [1993] 1W.L.R. 1083.
[40] Ibid.
[41] Further, see Odry, *op. cit.,* pp. 145-146.
[42] *Horne v Midland Railway* (1872-1873) L.R. 8 C.P. 131 at pp. 135-142 and pp. 146-148.

the defendant (the bank) that it is taking the risk of being liable for consequential losses.[43] Arora[44] confirms thus:

> "…unless the paying bank is made aware of the essential character of the prompt payment when it accepts the customer's instructions, the bank will not normally be liable for special loss which its customer suffers because the payment is essential to secure a contract he is negotiating….. If the bank is unaware of the need for prompt payment, the paying bank will not be liable to compensate its customer for the loss he suffers as a result of any special circumstances which necessitated the prompt payment."[45]

It is however extremely difficult for the courts to establish a clear view of whether the damages were in the parties' reasonable contemplation when they signed the contract.[46] In *Victoria Laundry (Windsor) Ltd v Newman Industries Ltd*,[47] Asquith L.J. held that the measure of damages recoverable in any case of breach of contract must depend upon first, "the loss actually resulting as was at the time of the contract reasonably forseeable as liable to result from the breach".[48] Secondly "what was at that time reasonably so foreseeable depends on the knowledge then possessed by the parties or, at all events, by the party who later commits the breach". [49] Accordingly, the defendant's knowledge of the special circumstances is of two kinds; one imputed, the other actual. Imputed knowledge is the knowledge of the reasonable person who is taken to know what loss is liable to result from a breach of contract in ordinary circumstances. This loss is the subject matter of the first rule of *Hadley v Baxendale.* But, the actual knowledge is the knowledge of special circumstances outside the

[43] McGregor, *op.cit*., at p. 26.
[44] Arora, *Electronic Banking and the Law, op.cit.,* p. 72.
[45] *Ibid.*
[46] *Simpson v London & North Western Railway Co* (1876) 1 Q.B.D. 274; *Seven Seas Properties Ltd v AL-Essa (No.2)* [1993] 1W.L.R. 1083; *Horne v Midland Railway* (1873) L.R. 8 C.P. 131; *Saint Line v Richardsons Westgarth& Co Ltd* [1940] 2 K.B. 99; *Victoria Laundry (Windsor) v Newman Industries* [1949] 2 K.B. 528.
[47] *Victoria Laundry (Windsor) v Newman Industries* [1949] 2 K.B. 528.
[48] *Ibid.*, at p. 539.
[49] *Ibid.*

"ordinary course of things" where losses resulting from a breach of contract are subject to the second rule of *Hadley v Baxendale.*[50] Thus one can conclude that in *Victoria Laundry (Windsor) Ltd v Newman Industries Ltd,* the court reached a result similar to that which was held in *Hadley v Baxendale*, namely the recovery for those losses that were foreseeable by a reasonable person as arising naturally in the usual course of things from the breach.[51]

In the context of consequential damages for recoverable EFT losses, since EFT is usually issued to settle commercial transactions, the paying bank, therefore might be considered to be cognizant of the possibility that the customer will sustain some commercial damages if the EFT instruction is executed incorrectly.[52] Moreover, Arora argues that the customer must be entitled to recover the losses which normally issue due to commercial payment not being made. Finally, he confirms that "usual commercial loss" is difficult to determine by the courts because as yet there is no method for calculating such damages.[53]

Given the above position, it seems that in EFT transactions, although the paying bank identifies that the main aim of payment instruction is to pay for the customers' commercial business, this is not an indication that the payer's bank acknowledges the consequential losses the customer may suffer if the EFT instruction is not executed correctly. Furthermore, with the growth of EFT transactions, a vast number of instructions are received every day by paying banks. These instructions should be carried out at high speed, thus it is very

[50] *Ibid.*
[51] Saidov, D., and Cunnington, R., *Contract Damages* (2008), p. 72.
[52] Arora, *Electronic Banking and the Law, op.cit.,* p. 72-73.
[53] *Ibid.*

difficult for the bank to expect the consequential losses for each payment instruction. Therefore, to consider the bank is liable for the consequential losses that the customer may suffer if the EFT instruction is not executed properly, the bank should be aware of such losses, and the matter falls within the second rule of *Hadley v Baxendale*. Furthermore, the bank must be aware of such potential consequential losses at the time of starting the contract, if the consequential losses of some EFTs exceed the losses which are brought to the attention of the bank at the time of signing the contract.[54] Accordingly, the customer should bring to the attention of the bank any potential consequential losses that may result if his transaction is not executed correctly. Currently, most banks include in their contract with the customer an express term to exclude their liability for consequential damages, such as delays or failures caused by industrial action, problems with another system or network and data processing failures.[55]

6.3.2.1 Recoverability of Currency Exchange Damages

Within EFT systems, currency exchange losses may happen in electronic credit transfer transactions,[56] while no such losses arise in EFTPOS and ATM transactions. Damages result from foreign exchange rate fluctuations between

[54] *Report by the Review Committee on Banking Services: Law and Practice*, ("The Jack Report") (1989, London, HMSO, Cm 622), p. 155, which the Review Committee recommended that a bank should be liable to its customer for direct or clearly consequential losses caused by EFT equipment failure.

[55] HSBC, *General terms and conditions*, 2012, section 11.6 http://www.hsbc.co.uk/content_static/en/ukpersonal/pdfs/en/personalbankingterms_conditions.pdf;
Lloyds TSB, *Your banking relationship with us,*2012, section 16 http://www.lloydstsb.com/assets/media/pdfs/banking_with_us/personal_banking_terms_and_conditions.pdf [20 April 2013].

[56] Lucia, J. S. S., 'Exchange losses from international electronic funds transfers: time to unify the law', (1988) 8 *Northwestern Journal of International Law & Business* 759 at p. 764.

the time at which an amount should have been transferred and the actual time taken for the transfer, where there is a delay or failure in execution of the payer's EFT instruction.[57] The risk is known as 'Herstatt risk'.[58] As explained in chapter four, there are several points which must be taken into account between the time the transfer is executed and the time when the payee receives payment that might be considered time of completion of payment. These points are: first, the time the payer's bank transmitted the payer's instruction. Secondly, the time the payee's bank receives the payment instruction. Thirdly, the time when the payee's bank acts on the payment instruction and the payment becomes irrevocable. Fourthly, the time when the payee's account actual credited with the transaction funds.

The problem of the finality of EFT extends beyond the determination of losses to the question of which party is liable to the payer. Determining the time of EFT payments is considered to be an important element in allocating an EFT party's liabilities for exchange rate fluctuation losses under a uniform rule.[59] There is an association, in calculating exchange losses, between the exchange rate at the time of the expected funds transfer and at actual time of the funds transfer. Determining EFT finality alone prescribes only the actual amount paid. However, since the exchange rate is different between the time of expected and actual payment, the exchange rate must still be determined.[60] As a result of the determination of the time at which the EFT is considered completed, the court is directing attention to the obligations of each of the EFT parties throughout the

[57] *Ibid.,* at p. 760.
[58] Cox, R. and Taylor, J., 'Funds Transfers', in Brindle, M. and Cox, R., *Law of Bank Payments* (2010), p. 76.
[59] *Ibid.*, at pp. 761-762.
[60] *Ibid.*, at p. 762.

course of the transfer. One question that needs to be asked, however, is whether the customer who suffers losses as a result of a subsequent variation in the exchange rate is entitled to claim damages for the loss sustained. Foreign currency loss recovery depends on the contemplation of the parties. Under English law where such loss was predictable, at the time of signed the contract, it is allowed to be recovered.[61]

President of *India v Lips Maritime (The Lips)*[62] is considered to be the case which dealt with the issue in the most comprehensive manner. In this case, Greek owners chartered their vessel to the charterer under a charterparty which provided that if the ship was detained beyond the lay days, demurrage should be paid at the rate of U.S. $6,000 per day (clause 9 of the charterparty). The amount of demurrage was to be paid in British Sterling at the exchange rate ruling on 1 July 1980 (clause 30 of the charterparty). The vessel completed discharge of the cargo on 11 October 1980. The owners claimed to recover, as damages for late payment of the outstanding demurrage, the loss suffered by them by reason of Sterling having depreciated by the date of the award.[63] At the arbitration stage, the umpire's decision, as interpreted by the Court of Appeal, was that the currency exchange loss suffered by the owners was “special damage” recoverable under the second rule of *Hadley v Baxendale,* and that the owners’ claim for damages was not precluded by the determination of the rate of exchange provision in clause 30.[64] The Court of Appeal based on the issue that the clause 30 did not apply when the paying party was in breach of

[61] *Di Ferdinando v Simon Smits and Co Ltd* [1920] 3 K.B. 409 at p. 416; *Ozalid Group (Export) Ltd v African Continental Bank Ltd* [1979] 2 Lloyd's Rep. 231.
[62] *President of India v Lips Maritime Corp (The Lips)* [1988] A.C. 395.
[63] *Ibid.*, at p. 395.
[64] Mann, F. A., ’Recovering currency exchange losses’, (1988) 104 *Law Quarterly Review* 3 at p. 3.

contract by failing to pay within two months of completion of discharge. The case further went to the House of Lords, which rejected the Court of Appeal approach. Lord Brandon held: [65]

> "All that happened was that the charterer did not pay liquidated damages for the detention of the ship at the time when the cause of action in respect of such damages occurred, or indeed at any time up to and including the date of the umpire's award. For that non-payment the only remedy which the law affords to the owners is interest on the sum remaining unpaid."[66]

Lord Brandon recognised that losses in this case cannot be increased by the award of further losses for currency exchange losses. That is because "claims to recover currency exchange losses as damages for breach of contract, whether the breach relied on is late payment of a debt or any other breach, are subject to the same rules as apply to claims for damages for breach of contract generally".[67] Therefore, it appears that the House of Lords did not exclude recovery of currency exchange losses as damages in other types of breach of contract if they are not too remote.[68] In this case, the House of Lords held that no exchange losses were recoverable because the damages are available for late payment of a debt but not for late payment of damages.[69] In this regard, currency exchange losses are recoverable as consequential damages, when such damages are within the contemplation of the parties at the time of signing the contract, under the second rule of *Hadley v. Baxendale*.[70]

---

[65] *President of India v Lips Maritime Corp (The Lips)* [1988] A.C. 395 at pp.425-426.
[66] *Ibid.*, at pp. 425-426.
[67] *Ibid.*, at p. 424.
[68] Mann and Brand criticising analysis of the House of Lords' decision, see respectively Mann, *op. cit.*, pp. 5-6 and Brand, R. A., 'Exchange loss damages and the uniform foreign-money claims act: the emperor hasn't all his clothes', (1992) 23 *Law and Policy In International Business* 1 at 48-49.
[69] *President of India v Lips Maritime Corp (The Lips)* [1988] A.C. 395; Further, see Saidov and Cunnington, *op. cit.,* pp. 487-488.
[70] *Hadley v Baxendale* [1854] 9 Ex. 341 at p. 356.

In EFT transactions, there are no statutory provisions relating to the recovery of currency exchange losses which could conflict with any right of recovery at common law. Thus, common law rules apply. It is the foreseeability of losses, both general and special, that governs recovery in the law of contract damages.[71] In this regard, the recovery of currency exchange losses suffered as a result of late payment is allowed under either rule of *Hadley v. Baxendale*, if the necessary principles are satisfied.[72] Thus, in the EFT transaction, recovering currency exchange losses depends on the contemplation of the parties at the time of initiating the transfer of funds, which is based on the facts of each case. The author's view is that in the EFT transactions losses arising from differences in currency rates may possibly occur, nevertheless it is problematic for banks to predict which currency will depreciate. Therefore, there should be no assumption that the bank is aware of such losses. A customer must prove that currency rates losses were in the contemplation of his bank as possible to result from a delay in the transfer of his fund at the time of sending his payment instruction.

This section contends that to determine whether there is currency liability for exchange losses, the court must first determine whether both parties in the EFT transaction intended currency exchange to be involved in the funds transfer. If so, the court should be clear that the delay in payment resulted in failure to exchange the funds at a favourable exchange rate, thereby causing exchange loss. The court must thus determine if there was a delay and if so which party was at fault. In contrast, if the court determines that the payee intends no

[71] Brand, *op. cit.,* p. 46; Saidov and Cunnington, *op. cit.,* p. 486 and p. 495.
[72] *Sempra Metals Ltd v Inland Revenue Commissioners* [2008] 1 A.C. 561; *International Minerals & Chemical Corp v Karl O Helm AG* [1986] 1 Lloyd's Rep. 81.

currency exchange upon the funds transferred there should be no currency exchange damages. The following pages are devoted to arguing that there is uncertainty in the recoverability of consequential damages within EFT transactions and thus it necessary to regulate or at least to establish proposal rules for covering such damages.

6.3.2.2 The validity of the applicability of common law rules of consequential damages in EFT transactions

One of the significant findings to emerge from this section is that the paying bank's liability to recover consequential damages in EFT transactions is uncertain and that this uncertainty may cause concern in the banking sector. This is possibly an issue which needs to be resolved by the banking sector, especially in the absence of judicial identification of the ambit of the applicability of common law rules in EFT transactions. This concern stems not from the recovery of consequential damages but from the uncertainty that surrounds the requirements of consequential damages recoverability. This arises from problems such as the difficulty in distinguishing between what constitutes an "imputed knowledge" and what are the "special circumstances" in order to identify whether or not the bank has contemplated such losses, and is thus under liability to recover consequential losses.[73]

As explained in the previous chapters, within common law rules it is the bank which bears the liability for any failure, fraud or negligence of the correspondent

[73] McGregor, *op.cit*., pp. 218-219; Saidov and Cunnington, *op. cit.,* p. 495.

or intermediary bank in executing the EFT transaction, although the banks in their standard term contracts can exclude or limit their liability for any failure or defaults in executing the payment instruction due to employees of correspondent or intermediary banks. Thus the customer who suffers losses in certain circumstances has no right to pursue the intermediary bank because there is no privity of contract between them and thus the intermediary bank owes no liability to the payer, even if the customer draws the attention of his bank to the “special circumstances”, at the time of issuing the EFT instruction to recover any consequential damages. This could be justified as the customer’s bank did not transfer the “special circumstances” to its agent (intermediary bank), as passing on such circumstances in the funds transfer system is impractical and costly and may hinder the high speed of the funds transfer. This leaves the customer without any remedy to recover either the direct damages or consequential damages from either the customer’s bank or the intermediary bank.

In view of the situation described above, this chapter argues that the bank’s responsibility for either the direct damages or consequential damages should be regulated by particular rules specific to EFT. One part of the problem could be solved by amending the PSR 2009 and establishing clear rules for the governance of direct and consequential damages. One of the more significant findings to emerge from this study is that there is a need for model rules which allocate rules of risk of direct damages and consequential damages. Within consequential damages there are a number of important issues which need to be addressed. Moreover, the rules allocating risk in currency exchange loss

must include fundamental definitions.[74] These include the following: (1) the liability of each party to the EFT must be defined in order to determine which party is responsible; (2) clarification of whether there is exchange liability or not; and (3) establishing the circumstances under which each exchange rule would be applied to achieve the most equitable result.[75] Such an approach could be adopted by SWIFT as the latter deals with international EFT's. The conclusion reached in this research, that there are no particular rules covering consequential damages, supports the suggestion that there is a need for 'model rules' which would offer several advantages in addressing the recovery of exchange damages sustained in delayed EFT transactions. These advantages are: first, creating more confidence in foreign exchange rate dealings via EFT systems; secondly, a reduction in the delay involved in funds transfer, as banks would be liable in respect of exchange rate loss; thirdly, a reduction in the need for parties to resort to litigation as clear rules governing liability develop over time; fourthly, in conclusion, the fact that the customer who sustained losses as a result of foreign currency exchange rate would receive reimbursement for delayed funds transfers would serve to foster efficient techniques and improvements in the EFT transactions. In this regard, the 'model rules' would determine the exact points at which each party is liable and that will based on time of payment. Ideally, the rules should establish that:

1- The payer should be liable for any foreign exchange rate losses happening between the time of issue of the payment instruction and the time of acknowledged receipt on the part of the payer's bank.

[74] Lucia, *op. cit.,* p. 778.
[75] *Ibid.,* at pp. 778-781.

2- The payer's bank should be liable for any foreign exchange rate losses occurring between the time of its receipt of the payment instruction and the time of transmitting the instruction to the payee's bank which has the opportunity to accept payment;[76]

3- The payee's bank should be liable for any foreign exchange rate losses occurring between the time it received the payment instruction and had the opportunity to accept payment, and the time at which it actually accepted payment.[77]

6.4 Conclusion

If the paying bank debits the customer's account outside the customer's mandate, the bank breaches its contractual duty to the customer to adhere to the customer's payment instruction. Breach of contract activates the paying bank's responsibility for the damages the customer bears, whether as a result of any unauthorized debiting of his account or as a result of a delay in payment. Such damages could be direct damages, consequential damages, interest loss or currency exchange losses. The recoverability of these losses is subject to the remoteness rule of *Hadley v Baxendale*,[78] which classified damages as either direct damages or consequential damages. There are no particular rules governing the banks liability for consequential damages. EFT is used to make commercial transactions, which means the customer's bank is aware that the customer uses EFT for commercial purposes, although such awareness is not

[76] *Ibid.* at p. 779.
[77] *Ibid.*
[78] *Hadley v Baxendale* [1854] 9 Ex. 341.

considered to be awareness of the special circumstances that the customer will bear commercial damages. The absence of particular rules covering consequential damages hinders the banks from executing the customer's payment instruction at high speed and low cost. In practice, a bank excludes or limits its liability for unauthorized EFT transactions carried out due to the intermediary bank's lack of care. One of the common law rules is that if there is no contract there is no case and therefore the customer does not have the right to sue the intermediary bank as there is no agreement between them. Due to this, the customer cannot claim for direct damages or consequential damages from either bank. It is the author's view that it is of the utmost importance that the UK legislation pays more attention to this process of damage recoverable within the EFT in order to accord higher protection to the customer. In addition, the bank's liability for direct and indirect damages should be determined by specific rules related to EFT.

Chapter Seven

Conclusion

Although, in recent times EFTs have grown in importance owing to their internet use on a global scale for commercial and financial transactions, there is no set of comprehensive legal mechanisms in the UK to supervise, monitor, and appropriately govern them. There are numerous uncertain issues in the current legal system against which EFT transactions are executed particular there is no comprehensive set of rules exist to cover the EFT parties' rights and obligations. Section 3 of the Bills of Exchange Act 1882 defines a bill of exchange as: 'an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay on demand or at a fixed or determinable future time a sum certain in money to or to the order of a specified person, or to bearer'. The 1882 Act which governs bills of exchange and provides for their legal implementation by such means as cheques, cannot be applied to EFT transactions, as the distinctive delineation of bills of exchange and promissory notes confines the scope of the Act to such devices.

English common law has defined a certain framework for the banker- customer relationship and the various circumstances in which that relationship is started and terminated. Definite implied terms have been added, to the banker-customer relationship, from time to time by courts, in cases where the contractual agreement failed to solve contentious issues. Usually the banker-customer relationship depends on implied contract, however an express

agreement is the basic ground in EFT transactions. The best example is payment by card transactions such as debit and ATM. The customer has no right to use such cards unless there is an express contract. In practice it is unusual to negotiate individualised contracts with the bank for each transaction; banks normally have their own uniform contracts. In general the EFT transactions are based on the banker-customer relationship and this is a particularly powerful and attractive idea. At some point, however, the contract runs out, and courts must address risks and liabilities which the parties have not foreseen or failed to address. English courts regard the legal nature of a payment instruction in a credit transfer transaction as an authority and mandate from a payer to his bank to transfer a sum of money to a payee's account.[1] It was held that such payment instruction is governed by the common law of agency.[2] It was noted in *R. v King*[3] that the effect of an electronic payment order executed via CHAPS was to "direct the paying bank to debit the paying customer's account with £x to the credit of the payee's account at another bank and to do so by means of an electronic device".[4]

Given the significance of the EFT system as a method of payment in the contemporary business world, one would imagine that the rules governing such a system would be highly advanced and would clearly allocate the accompanying risks to the parties involved. The Payment Services Regulations 2009 do, when it's applicable, but when it's not unfortunately, no such rules exist in the United Kingdom. The purpose of the current study was to examine

[1] *Royal Products v Midland Bank* [1981] 2 Lloyds Rep. 194 at 198 per Webster, J.
[2] *Ibid.; Libyan Arab Foreign Bank v Manufacturers Hanover Trust Co (No.2)* [1989] 1Lloyd's Rep. 608.
[3] *R. v King and Other* [1991] 3 All E.R. 705.
[4] *Ibid*., at p. 709 per Lord Lane; See section 2.5.3.4.

how the law allocates risks between the parties in relation to unauthorized payment, insolvency risk and privacy.

7.1 The flaws of the PSR 2009 in the context of the allocation of risks associated with EFT

A thorough examination of the provisions of the PSR 2009 indicates that they are limited in application, as they apply to funds transfers between banker and customer in the UK,[5] and, between the payer's bank and the payee's bank within the EEA,[6] covering EFT transactions denominated in Sterling, the Euro, and other European currencies.[7] Equally important, the PSR 2009 distinguish between different types of customers, namely consumer and business, and in this regard, when the customer is not a consumer the parties have the right to agree to not apply several regulations relating to Part 6.[8] Therefore PSR 2009 do not comprehensively regulate the rights, obligations and liabilities of the parties to the transaction (payer, paying bank, payee's bank, and payee) and their liabilities for unauthorized EFTs, non-payment, direct damages and consequential damages. The previous chapters have demonstrated that the PSR 2009, when it is applicable, are not without flaws and deficiencies. Thus, it fails to address all of the legal issues surrounding EFT transactions. The PSR 2009 provisions offer new rights to the customer with regard to the countermanding of payment instructions, implementation time and charges.

[5] PSR 2009, regulations 33(1)(a) and 51(1)(a).
[6] *Ibid.,* regulations 33(1)(b) and 51(1)(b).
[7] *Ibid*., regulations 33(1)(c) and 51(1)(c).
[8] *Ibid*., regulations 51(3)(a).

Furthermore, it stipulates that the funds must be made available to the payee by crediting the payee's account with a certain time period. Nevertheless, this leads to problems when the payee's account is overdrawn. The PSR 2009 fails to define the exact time of EFT finality and raises other problems without providing answers to them, for example: (a) the meaning of availability with regard to funds; (b) the issue of acceptance of the EFT instruction by the payee's bank and the extremely important question of when the inter-bank EFT payment is deemed final; (c) the meaning of defective execution; (d) the funds discharged; and (e) the wrongful or non-exist a payee.

The PSR 2009 present no solution to the problem of identity authentication and its effect on the parties' liability for an authenticated but unauthorized EFT instruction. It does not specify which party should be liable for an authenticated but unauthorized payment instruction carried out by one of the payer's employees, or by one of the paying bank's employees, or by a third party. Furthermore, it contains no provisions for determining the standard of the security procedures which should be employed by the banks in the context of EFT. If the customer suffers any loss of money due to an unauthorized transaction, the PSR 2009 decree that the bank must refund the amount of the transaction with interest; but such a remedy is not available in the case of losses caused by delay or non-payment. The regulation of the EFT parties' relationship by different forms of law, namely the PSR 2009, agency law and contract law, causes more confusion for both parties in the EFT transaction as their liabilities may be treated according to different sets of rules. The absence of a comprehensive framework governing the banker-customer contractual relationship with regard to rights, obligations and liabilities for unauthorized risk,

non-payment risk and confidentiality risk, together with the existence of different sources, leads to unpredictability, uncertainty and unfair treatment for both parties.

7.2 Allocation of unauthorized risk and the problem of identity authentication

The authorization of banks to execute EFT transactions on behalf of their customers is one of the important issues in the banker-customer relationship. Banks' liability for unauthorized EFT payment depends on whether such payment is authorized or not. There is an important connection between identity authentication and the authorization of electronic payment instructions. [9] Chapter three[10] has demonstrated that in an electronic payment instruction the absence of physical meeting between the bank and customer means that the bank has no capacity for determining and identifying the person who issued the payment instruction. There is therefore normally a term in the banker-customer contractual agreement which specific security procedure according to which a customer's electronic payment instructions will be tested. After the payment instruction is tested by passing the security procedures the payment instruction is an authenticated payment instruction. Although, using agreed security procedures present no final solution to identify the person who issues the payment instruction, or establish whether he was in fact authorized to do so or not. Applying the rules of agency law, contract law and the rules applying to

[9] For more detail see chapter three, section 3.3.1.
[10] *Ibid.*

forged cheques to an authenticated payment instruction leads to uncertainty and unpredictability.

The common law provides that a bank is not entitled to debit its customer's account unless the customer has authorized it to do so.[11] Where a bank acts without customer mandate and debits its customer's account on the basis of an unauthorized instruction, the customer is entitled to claim for re-crediting his account with the transaction funds and the interest on those funds.[12] Where an unauthorized transaction is passed the bank may seek to make the customer liable. A customer is under a duty to inform his bank immediately he becomes aware of the unauthorized transaction. Otherwise he may be found liable for facilitating a forgery if a customer fails or delays to notify the bank about the unauthorized transaction. A bank may plead that its customer is estopped from asserting that the bank is not entitled to debit his account.[13] Regarding the PSR 2009 the customer is under an obligation to inform his bank 'without undue delay' upon becoming aware of the unauthorized nature of the transaction, and this can never exceed 13 months from the date when the payer was debited with the payment.[14] Finally a customer may be found liable for an unauthorized transaction if the payer's bank can prove that he acted fraudulently or negligently. The paying banks may seek to avoid liability for authenticated but unauthorized payment instructions by including term in their contracts with the customers that exclude or limit their liability for such payment instructions.[15] This leaves the customer with an unfair contract terms, and makes him liable for

[11] See chapter three, section 3.4.2.
[12] For a fuller discussion, see chapter six.
[13] See chapter three, section 3.4.1.2.
[14] PSR 2009, regulation 59(1) and regulation 51(3)(b).
[15] Chapter three, section 3.3.2.2.

an authenticated but unauthorized payment instruction created by a third party. it is unfair for the customer to bear the liability for an authenticated but unauthorised payment instruction when such instruction created by a third party without the customer's negligence. The bank is obliged to provide sufficient security procedures and thus an offender who obtains the customer's security procedures without the customer's negligence, the bank is liable for authentication but unauthorised transaction, not the customer. The bank bears the losses because such authenticated but unauthorized transaction accrued as a result of the technology that the bank makes its customers use. The customer bears no liability for failing to deal with such risks, because these are risks under the control of the bank. Taken together, these findings suggest that the rules governing paper-based payment orders are no longer adequate for the regulation of the rights, obligations and liabilities of banks and their customers and that there is a need for the formulation of a new set of applicable rules.

The validity of security procedures is regulated by the Electronic Communications Act 2000 and the Electronic Signature Regulations 2002, irrespective of the kind of electronic transactions for which they are used. These provisions establish the legal framework for e-signature and certification authority services. They account for the fact that simple and advanced signatures are, in fact, acceptable and valid in legal procedures.[16] This study has shown that, in the context of EFT, the effect of the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002 has been to make the security procedures acceptable in evidence and also to prove the authenticity of the communication or data, or the integrity of the

[16] *Ibid.,* section 3.3.2.3.

communication or data. However, the legal effect of electronic signatures on the payer or the payer's bank's liability for any unauthorized payment instruction is not addressed and is, accordingly, left to the court's discretion. Taken together, these results suggest that the following points should be taken into account when the rules are formulated in the context of EFT transactions, viz:

1. The current law presents the customer's right to authorize payment instructions only through explicit consent. While the author's recommendation is that the rules should give the customer the right to authorize payment instructions through either explicit or implicit consent.

2. The rules should place the customer under a duty to protect and safeguard his security procedures and to protect and safeguard the computer terminal from attack by hackers and others. Taking into account a customer is liable if he fails to inform his bank about any unauthorized transaction as soon as he becomes aware of such a transaction.

3. It is reasonable and fair practice establishes rules which place the customer who acts without fault under no liability to bear any losses resulting from unauthorized instructions and the bank should bear all losses, even if it has acted without fault.[17]

4. The rules should place emphasis on the bank's duty to carry out reasonable security procedures.

[17] Geva, B., 'Consumer liability in unauthorized Electronic Funds Transfers', (2003) 38 *Canadian Business Law Journal* 207 at pp. 280-281.

7.3 Allocation of credit risk and the problem of EFT finality

A payment instruction constitutes only a mandate and from this two consequences arise: First, the payer has the right to revoke the payment instruction unless it has been executed. Second, the payee has no right to the money transferred until the payment order is completed. In EFT transactions, completion of payment means the time at which the funds transferred are actually credited in the payee's account and can be used by the payee as equivalent to cash. On the question of general rules, and with an absence of statutory guidance, the common law has investigated 'payment finality' and seems to have recognised two positions;[18] depending on whether the transfer is "intra-bank" or "inter-bank". For intra-bank transfers, courts acknowledge finality as the time at which the payer's bank, or its agent, receives the payment instruction.[19] It was held in *Momm v Barclays Bank International Ltd*[20] that payment had been completed when the "decision" to transfer the funds was irrevocably taken by the bank by setting the appropriate computer process in motion.[21] In contrast, for inter-bank transfers, the courts have recognised that the point of finality is when the payee is informed by his bank of the receipt of the transaction funds and these funds are actually credited to the payee's account.[22] English law 'settled' that the 'finality of payment' takes place when one of the following events occurs: the first event is payment by the payee's bank to the payee, usually by crediting the payee's account with the transaction

[18] For a fuller discussion, see chapter four, section 4.3.3.
[19] *Mardorf Peach & Co Ltd v Attica Sea Carriers Corp of Liberia (The Laconia)* [1975] 1 Lloyd's Rep. 634; [1976] Q.B. 835; [1977] A.C. 850.
[20] *Momm v Barclays Bank International Ltd* [1977] Q.B. 790.
[21] *Ibid.,* at pp. 881-882.
[22] *Rekstin v Severo Sibirsko AO* [1933] 1 K.B. 47 at p. 57.

funds, regardless of whether the payee has been informed of the transfer.[23] The other event is payment by the paying bank to the payee's bank.[24] The determination of the time of occurrence of the second action, that of payment by the paying bank to the payee's bank, depends on the method of payment. Accordingly, EFT payment finality takes place when the payee's bank accepts the payment instruction from the payer's bank and agrees to credit the payee's account with the transaction funds, regardless of whether the payee's bank has actually credited the payee's account and regardless of whether it has informed the payee of the transfer.[25]

Payment is presumed to be final for the payer when the payer's bank obligates itself irrevocably to that payment, while payment is presumed to be final for the payee when the payee's bank obligates itself by accepting the payment. In this thesis it has been argued that a customer who opens an account with a bank necessarily bears the risk of that bank's insolvency. Thus the payer will be liable for the payment before the fund transfer transaction in the case of his bank's insolvency but after the fund transfer transaction is made it is the payee who bears the risk of that insolvency.[26]

Given the above exposition, it seems that the finality of EFT is at the destination bank in the relevant system. In a credit transfer the payment operation will be completed at the payee's bank. Conversely, in a debit transfer the payment operation will be completed at the payer's bank. Generally, the identity of the payee should be firmly established in the payment instruction; otherwise the

[23] Chapter four, section 4.3.3.1.
[24] Chapter four, section 4.3.3.3.
[25] *Ibid.*
[26] *Ibid.*, for a fuller discussion, see section 4.5.

destination bank must reject the instruction. Any agreement between the parties should also be taken into consideration.[27] The proposed model for EFT finality rules is as follows:

First, the credit transfer instruction becomes final when the payee's bank is paid.

1. In intra-bank transfers the credit transfer instruction is paid once the payer's bank has debited the payer's account. Thus, the payer has the right to revoke the payment instruction as long as his bank has not taken any action to execute the payment instruction; conversely, the payer has no right to revoke the payment instruction once his account has been debited.

2. In an inter-bank transaction, the credit transfer instruction is paid when the payee's bank, with the payee's actual or ostensible authorization, has accepted to make the transfer on the payee's behalf. The payee's bank's approval to make payment is shown by either (a) crediting the payee's bank account, or (b) by actually crediting the payee's account enabling the payee to use the funds in same way as cash. The payer has the right to revoke the payment instruction as long as the payee's bank has not accepted the instruction. Acceptance by the payee's bank of the credit transfer instruction makes the payment final and irrevocable.

3. Completion of the credit transfer instruction makes the destination bank indebted to the payee as with a transaction fund. However, crediting the payee's account and enabling the payee to use the funds transfer as cash may not be permissible in cases where: (a) the payee's account is

[27] *Customs and Excise Commissioners v National Westminster Bank Plc (Authorisation: Mistake)* [2002] EWHC 2204.

overdrawn; or (b) there is an agreement between the payee and the payee's bank that the payee has no right to use the transaction funds until the payee's account has actually been credited by the payer's bank.

Secondly, finality of debit transfer instructions is when the payer's bank has debited the payer's account and has not reversed the debit or refused to make the payment:

1. The value date of the debit transfer instruction is considered final at the end of the day where the payment instruction is received, even if there is no actual debit to the payer's account, assuming that the payer's bank has accepted to make the fund transfer.

2. The debit transfer instruction will not be considered final if the payer's bank has reversed the debit or refused to make the payment. The bank must take this decision between the time of receiving the payment instruction and the end of the day on which the payment instruction was received.

3. The payee has the right to revoke the payment instruction between the time of the receipt of the payment instruction by the payer's bank and the end of the day following that on which the payment instruction was received. At the end of the day following the day on which the payment instruction was received the payee has no right to revoke the instruction and the debit transfer is to be considered final. Such a period is to ensure that the payer has been notified of the payment instruction.

4. Completion of the debit transfer instruction makes the payer's bank liable to the payee's bank for the transfer of the funds within a time not exceeding the end of the day following the day on which the payment instruction was

received. After receiving the funds, the payee's bank will in turn be liable to the payee for the funds transaction. At that point, any provisional credit provided to the payee is to be considered final.

5. In a debit transfer instruction the payment is considered final and the payee's bank is liable to the payee for the payment if the payer's bank has debited the payer's account and transferred the funds to the payee's bank, even if the payee's bank has faulty data or experiences telecommunication problems

7.4 Privacy and the problem of disclosure to CRAs

A recurring issue in EFT systems is how to create an acceptable level of consumer trust and confidence. As explained previously, the banker-customer relationship in EFT transactions is an agency contract and the element of privacy stems from this contract. Generally, an agent is under a duty of care and privacy to his principal.[28] The principles of a bank's duty of confidentiality were identified in *Tournier v National Provincial and Union Bank of England*.[29] The *Tournier* principles, however, left some issues unsolved. One of the Jack Committee recommendations was that a standard of best practice should require that, at the beginning of the bank-customer relationship, the bank should explain and describe very clearly how the banking system works and should invite customers to give or withhold a general express approval for their banks

[28] *Regal (Hastings) Ltd v Gulliver* [1967] 2 A.C. 134; *Boardman v Phipps* [1967] 2 A.C. 46.
[29] *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461 at 427.

to submit opinions on them in response to status enquiries.[30] However, the bank has the right to establish a term in its contract with the customer entitling it to disclose information concerning a customer's creditworthiness. This thesis has argued that the doctrine in *Turner*'s case presents a clear explanation in the area of implied consent theory.[31] In this regard, the best recommendation is that the principles governing the bank's duty of confidentiality should be regulated by statute in order to avoid any ambiguities. Given the above position, it seems that the implied consent theory has been changed, since the Court of Appeal in *Turner* held that the bank has no right to disclose or exchange customer's confidential information on the basis of the customer's implied consent. Although, implied consent may exist in particular cases, its scope is very limited. Therefore, banks need to be extremely careful when relying on implied consent as a basis for disclosing customer information. Overall, it is fair practice to obtain the customer's express consent before passing any confidential information to another party and if the bank fails to do so it will be liable for breach of a duty of confidentiality.

Scant attention has been paid by government to some significant issues, namely the ambiguity surrounding the disclosure and exchange of customer data with the CRAs. Therefore, there is lack in the academic references in this subject. A connected argument is that credit data exchanges through CRA's are executed in the interest of the parties involved. Banks depend on customer approval, which could be either express or implicit when customer's data is given to CRA's. This thesis argues that the disclosure of a customer's

[30] *Report by the Review Committee on Banking Services: Law and Practice, op.cit*., p. 49.
[31] *Turner v Royal Bank of Scotland Plc* [2001] EWCA CIV 64.

confidential information to the CRAs is illegal unless the bank obtains the customer's express authority for such disclosure.[32] Therefore it would be desirable to have a set of model rules, or at least a code of practice, which regulates these points and clarifies with precision the principles and conditions by which a bank can exchange information with CRAs. Such a model is needed to clarify and protect a customer's private data and to balance a customer's right of confidentiality with the public interest in data disclosure and with the disclosure by compulsion of law.

Thus, the proposal for an approval model the author's recommendations in this thesis is as follows: First, the model should include the bank's procedures for notifying the customers as to how it might use their data, regardless of whether it is positive or negative, and should not exchange any customer information without the customer's express approval.

1. Before customers sign a contract involving an EFT system, the banks must provide them with a privacy notice written in understandable and clear language, explaining the conditions under which the EFT data, whether negative or positive, will be exchanged and disclosed to the CRA's.

2. That privacy notice should explain how the bank will use and protect customer information.

3. The bank should obtain a new consent from the customer if there is any change in the terms and conditions of the privacy notice.

[32] *Ibid.*, section 5.4.4.1.

4. The bank must use customer data for exclusive purposes and according to the reason for its collection, such as for making debit or credit transactions. Further, data processing should be with significant protection and under internal control or direct supervision.

5. The customer should have the right to refuse to sign the notice and the right to refuse the bank permission to exchange and use his data without any effect on the customer-banker relationship. Currently most banks offer online banking for their customers. As a result, registered internet banking customers must accept the bank's terms by exercising 'tick-box' which enable the customer to exercise most banking transactions via the internet, for example, make payment, drawing cheques or transferring bank. Internet banking has developed that promises great advantages to banks and customers. Customers will adopt the online banking if they believe the system will bring advantages such as saving time by not physical visiting to bank and protect their confidential data. Online banking services will not process unless ticks the box to accept the bank's terms. That leaves customer without any right to refuse any bank's terms as the computer will not process customer transactions unless accept the general terms and condition by click on the particular box to accept the bank's terms. Thus, even with the online banking the customer should have the right to refuse the bank’s permission to exchange and use his/her data without any effect on the customer-banker relationship

6. In the case of the customer’s refusal to give the bank general approval to disclose and exchange his data, the bank should obtain the

customer's express approval each time the bank wants to exchange its customer data.

7. The bank must clarify to the customer what a CRA is and in whose interest exchanged is the data.

Secondly, there must be an emphasis on the voluntary nature of the disclosure of the customer's data to the CRA's. Such disclosure must be regulated and must be specific to particular data, with unlimited disclosure being unacceptable. Furthermore, it is essential also to regulate the CRAs and the ways in which they use and protect a customer's private information. Thirdly, the bank must supply accurate customer data. Regarding accurate data, the CRAs should exercise reasonable care and skill in demonstrating the accuracy of data provided by the banks and should state the purpose for which they were exchanged and disclosed.

This thesis concludes that the existing confidentiality laws do not provide the customer with an adequate level of protection and safety for the control of the recording and exchange of data relating to EFT transactions. Thus, the model proposed in this thesis should assist in providing sufficient protection to the customer. Disclosure of a customer's data should be made to a third party only if it is necessary to the EFT procedure or for a purpose to which the customer has given express approval.

7.5 EFT, recoverability of damages and the problem of the validity of the applicability of common law rules of consequential damages

The banker-customer relationship in EFT transactions is contractual and the measure of damages is that which is applicable in breaches of contract generally, that is in absence of contractual agreement to the contrary. Thus, where a bank has not executed one of its duties toward the customer in an EFT transaction it will have breached its contractual duty to the customer. In such case, the customer should be put in the same position that he would have been in had the bank acted in accordance with its agreement and executed the customer's instructions properly. This is subject to the remoteness test developed in *Hadley v Baxendale*[33] and applied in later cases.[34] The general policy is that a customer is entitled to recover direct losses: his principal amount and interest losses thereon. Consequential damages which do not arise naturally are not recoverable, except where there is an express written agreement of the bank concerned.

It is argued that the position concerning the recoverability of consequential damages under English law for banks which fail to make a fund transfer correctly or delay or non-transfer of funds is unacceptable for both banks and customers. Under common law, consequential damages are not recoverable except when such damages a within the contemplation of the bank at the time

[33] *Hadley v Baxendale* [1854] 9 Ex. 341.
[34] The PSR 2009 which, when applicable, entitles the payer to request from the payer's bank a refund of the amount involved in the transaction if the bank made the payment according to an unauthorized instruction, regulation 61.

when it receives the payment instruction. The bank should have notice of the special circumstances that triggered the customer's losses at the time of received the instruction. Regarding the customers, a notice of "special circumstances" to the paying bank does not indicate that other banks in the payment system are a notice of "special circumstances". Transmitting such notice to each bank involves in the EFT system is obviously too difficult because EFT as a methods of payment designed to work in speed and low cost. Thus, when banks exclude or limit their liability for any failure or default in executing the payment instruction on the part of an employed correspondent or intermediary bank, the customer has no right to pursue the intermediary bank because there is no privity in contract between them. This leaves the customer without remedy for recovery of EFT losses. Regarding banks, the knowledge of "special circumstance" will make the bank liable for consequential a damage which is not necessarily to be actual knowledge but could be an imputed knowledge.[35] The ambiguity resulting from the interpretation of imputed knowledge may cause banks huge funds.

The existing non-specific rules covering the bank's liability for both damages are indeed risk needs to be clarified by some sort of express regulations. This risk could be either that there is unpredictability or uncertainty in the paying bank's liability due to the absence of an express agreement to carry out its liability; or the payer, as the weaker party, will bear the losses for non-payment or unauthorized EFT not executed as a result of his negligence or fault, where the paying bank has clearly expressed that it bears no liability for the particular kinds of risk associated with EFT transactions.

[35] *Victoria Laundry (Windsor) v Newman Industries* [1949] 2 K.B. 528, at pp. 539-540.

7.6 Recommendations

In the light of the examination of the existing law regulating EFT in the UK, the final question that should be addressed in this conclusion is whether there is a need to adopt a new independent body of law to govern EFT transactions. The Jack Committee raised this question and it was recommended that new rules for new technology were needed.[36] The significant argument against the necessity for a new body of law to govern EFT transactions stems from the fact that paper-based transactions and EFT transactions are only methods for transferring funds from one person to another. The dissimilarity in the standard that funds are transferred over does not affect the parties' rights and duties since the purpose in all payment system is to transfer funds over from one person to another. Therefore, the current rules can be covered to address issues arising specifically in EFT systems.[37] The case against the necessity for a new body of law to govern EFT transactions submits that where the common law and other payment systems rules fail, private contracts between the parties will usually fill the gap. The Unfair Contract Terms Act 1977 when the term is "unreasonable" and the Unfair Terms in Consumer Contracts Regulations 1999 when the term is "unfair" will guard customers against unreasonable and unfair terms. One of the more significant findings to emerge from this study is that there is a needing to adopt a new independent body of law to govern EFT transactions. Regulating EFT involves creating equilibrium between the predictability and certainty of the bank's liability for risks associated with EFT

[36] *Report by the Review Committee on Banking Services: Law and Practice*, ("The Jack Report") (1989, London, HMSO, Cm 622), paras. 9.29 to 9.31.
[37] *Ibid.,* at para. 9.14.

and the protection of the customer from unfair contract terms imposed by the bank. The new rules are needed not to cover issues resulting from the aim of the EFT systems but from the method of achieving such aim. Accordingly, the most convincing reason to legislate for EFT system is to redress any existing laws that create obstacles to EFT transactions. Such obstacles typically contain rules laying down requirements as preconditions to legal effectiveness. Such rules expressly or impliedly require a particular form, for example, authenticate customer's instructions in EFT transactions is completely different and raises different legal issues from an authentication of a cheque, on which the signature must be hand-written. The Bills of Exchange Act 1882 does not cover EFT system since its ambit of application is limited to paper-based transactions and not applicable to EFT transactions. Although, a thorough examination of the Payment Services Regulations 2009 reveals that its rules are insufficiently comprehensive since they do not regulate EFT transactions involving non-European currency exchanges. Since it is common law which regulates EFT transactions involving the legal problems described above, the author argues that there is a definite need for a new independent body of law to govern EFT transactions, replacing the rules that were created to regulate only paper-based funds transfers. This thesis is showed that the private contracts, including the rules of clearing and payment system, are insufficient and drafted to guard the interest of the banks. Furthermore, it is improbable under current conditions that banks and cards issuers such as VISA and MasterCard will choose of their own volition to set up a regime of reversibility granting chargeback rights to customers globally. To date, these banks and card issuers have not even gone so far as to extend universal chargeback rights to disputes relating to products

and services, as CCA 1974 section 84 did for many UK consumers who purchase with credit cards. Nevertheless, the problem arises where debit and prepaid cards are subject to disputes. Debit cards holders may face the risk of supplier misconduct as a result of the absence of particular and effective rules for the protection of customers; yet, overwhelmingly, in emerging economies payment card issuers and card associations are self-regulating. Finally, a new legislation may be to create confidence in the legal and commercial environment among customers and banks.[38] EFT transaction's parties could be given motivations to prevent guard against common risks such as fraud and insolvency. Failing to prevent a loss from occurring, a rule may either distribute the loss according to the degree of fault or allocate the loss to the party that has the last clear chance to prevent such loss from occurring but failed (may be negligently) to do so. Within any arrangement, wherever commercial legal issue take place between banks and their customers, inevitability of result is more significant than the ambiguity of classic litigation.

It is obvious that using EFT in banking circles create legal problems need more investigation and study to explain the difficulty which arising from using such systems. It is recommended that further research be undertaken in the following areas: the satisfaction of consumers with banks' services in EFT transactions, particular addressing legal issue over error or authentications procedures; the outlining of a Code of Conduct for CRAs; the success or failure of the PSR 2009 in practice may also be examined; and the outlining of a new policy for consumer protection.

[38] Smith, G. J. H., et al., *Internet Law and Regulation* (2007), pp.848-851; Bergsten, E. E., 'Legal aspects of international Electronic Funds Transfers', (1987) 7 *International Business Law* 649 at p. 652 and p. 655.

Bibliography

Books

Alastair, H., *The Law of Finance* (2009, 1st Edition, London, Sweet & Maxwell)

Andrews, G. M., and Millett, R., *Law of Guarantees* (2001, 3rd Edition, London, Sweet & Maxwell)

Arora, A., *Cases and Materials in Banking Law* (1993, London, Pitman)

Arora, A., *Electronic Banking and the Law* (1988, London, IBC Financial Books)

Atiyah, P. S., et al., *Atiyah's Sale of Goods* (2010, 12th Edition, Edinburgh, Pearson Education)

Bainbridge, D., *Introduction to Information Technology Law* (2008, 6th Edition, Edinburgh, Pearson Education)

Beale, H. G., et al., *Contract* (2008, 5th Edition, Oxford, Oxford University Press)

Beatson, J., et al., *Anson's Law of Contract* (2010, 29th Edition, Oxford, Oxford University Press)

Becker, E., et al., *Digital Rights Management* (2003, Germany, Springer-Verlag)

Blair, W., *Banks and Remedies* (1999, 2nd Edition, London, Taylor & Francis)

Blair, W., *Banks, Liabilities and Risk* (2001, 3rd Edition, London, Lloyd's of London Press)

Borrie, G. J., *Commercial Law* (1988, 6th Edition, London, Butterworths)

Brindle, M., and Cox, R., (eds), *Law of Bank Payments* (2010, 4th Edition, London, Sweet & Maxwell)

Burrows, A. S., et al., *Law of Restitution* (2007, 2nd Edition, Oxford, Oxford University Press)

Carty, H., *An Analysis of the Economic Torts* (2010, 2nd Edition, Oxford, Oxford University Press)

Caux, T., et al., *Electronic Banking and Treasury Security* (2000, 2nd Edition, London, Woodhead)

Charles, P., *The Law and Practice of International Banking* (2010, Oxford, Oxford University Press)

Chissick, K., 'An Introduction to Electronic Payment Mechanisms, Encryption, Digital Signatures and Electronic Surveillance' in Chissick, M., and Chissick, K., *Electronic Commerce, Law and Practice* (2002, 3rd Edition, London, Sweet & Maxwell)

Chitty, J. D., *Chitty on Contracts* (2008, 30th Edition, London, Sweet & Maxwell)

Chorley, L., *Law of Banking* (1974, 6th Edition, London, Sweet & Maxwell)

Chris, R., et al., *Cross-Border Electronic Banking: Challenges and Opportunities* (2000, 2nd Edition, London, Lloyd's of London Press)

Clarke, O., *A Practical Guide to E-Commerce and Internet Law* (2005, 2nd Edition, London, ICSA)

Collingwood, P., *PayPal in 30 Pages or Less* (2004, Canada, Timesaver Books)

Cranston, R., 'Law of International Funds Transfers in England' in Hadding, W., and Schneider, U. H., *Legal Issues in International Credit Transfers* (1993, Berlin, Duncker & Humblot)

Cranston, R., *Principles of Banking Law* (2002, 2nd Edition, Oxford, Oxford University Press)

David, W., *Cybercrime: The Transformation of Crime in the Information Age* (2007, 1st Edition, Cambridge, Polity Press)

Davies, I. R., *Commercial Law* (1992, London, Blackstone Press)

Dorn, J. A., *The Future of Money in the Information Age* (1997, Washington, Cato Institute)

Edelman, J., *Gain-Based Damages: Contract, Tort, Equity and Intellectual Property* (2002, Oxford, Hart)

Edwards, L., and Waelde, C., *Law and the Internet: A Framework for Electronic Commerce* (2009, 3rd Edition, Oxford, Hart)

Ellinger, E. P., 'Electronic Funds Transfer as a Deferred Settlement System' in Goode, R., *Electronic Banking: The Legal Implications* (1985, Institute of Bankers and Centre for Commercial Law Studies, Queen Mary College, University of London)

Ellinger, E. P., et al., *Modern Banking Law* (2011, 5th Edition, Oxford, Oxford University Press)

Ferretti, F., *The Law and Consumer Credit Information in the European Community* (2008, London, Routledge-Cavendish)

Fletcher, I. F., *The Law of Insolvency* (2009, 4th Edition, London, Sweet & Maxwell)

Frazer, P., *Plastic and Electronic Money: New Payment Systems and Their Implications* (1985, Cambridge, Woodhead-Faulkner)

Furmston, M. P., et al., *Commercial Law* (1995, London, Cavendish)

Geva, B., *Bank Collections and Payment Transactions* (2001, Oxford, Oxford University Press)

Geva, B., *Legal Aspects Relating to Payment by E-Money: Review of Retail Payment System* (2001, London, London Institute of International Banking, Finance & Development Law)

Geva, B., *The Law of Electronic Funds Transfers* (2003, New York, LexisNexis)

Gkoutzinis, A., *Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce* (2010, Cambridge, Cambridge University Press)

Goldspink, R., and Cole, J., *International Commercial Fraud* (2004, Volume 2, London, Sweet & Maxwell)

Goode, R., 'Electronic Funds Transfer as an Immediate Payment System' in Goode, R., *Electronic Banking: The Legal Implications* (1985, Institute of Bankers and Centre for Commercial Law Studies, Queen Mary College, University of London)

Goode, R., *Consumer Credit Law and Practice* (London, loose-leaf, Sweet & Maxwell)

Goode, R., *Goode on Commercial Law* (2009, 4th Edition, London, LexisNexis Butterworth)

Goode, R., *Goode on Legal Problems of Credit and Security* (2008, 4th Edition, London, Sweet & Maxwell)

Goode, R., *Payment Obligations in Commercial and Financial Transactions* (1995, 2nd Edition, London, Sweet & Maxwell)

Goode, R., *Principles of Corporate Insolvency Law* (2005, London, Sweet & Maxwell)

Griffiths, G., and Neate, F., (ed's), *Bank Confidentiality* (2008, 4th Edition, West Sussex, Tottel)

Guest, A. G., and Lloyd, M., *Encyclopaedia of Consumer Credit Law* (1974, London, loose-leaf, Sweet & Maxwell)

Guest, A. G., *Benjamin's Sale of Goods* (2006, 7th Edition, London, Sweet & Maxwell)

Guest, A. G., *Chalmers and Guest on Bills of Exchange, Cheques and Promissory Notes* (2009, 17th Edition, London, Sweet and Maxwell)

Hailsham, Q. H., et al., *Halsbury's Laws of England* (2010, 5th Edition, London, LexisNexis Butterworth)

Hapgood, M., et al., *Paget's Law of Banking* (1996, 11th Edition, London, LexisNexis Butterworths)

Hapgood, M., et al., *Paget's Law of Banking* (2007, 13th Edition, London, LexisNexis Butterworths)

Harris, D., et al., *Remedies in Contract and Tort* (2005, 2nd Edition, Cambridge, Cambridge University Press)

Haynes, A., *The Law Relating to International Banking* (2010, West Sussex, Bloomsbury Professional)

Hedley, S., *The Law of Electronic Commerce and the Internet in the UK and Ireland* (2006, 1st Edition, London, Cavendish)

Herring, J., *Criminal Law* (2008, 3rd Edition, Oxford, Oxford University Press)

Holden, J. M., *Law and Practice of Banking* (1991, 5th Edition, London, Pitman Publishing

Hollander, C., *Documentary Evidence* (2012, 11th Edition, London, Sweet & Maxwell)

Holloway, D., *Commercial Law* (1997, London, Old Bailey Press)

Hudson, A., *The Law of Finance* (2010, 1st Edition, London, Sweet & Maxwell)

Hudson, P., and Mann, J. E., *Commercial Banking Law* (1978, Plymouth, Macdonald and Evans)

Jones, M. A., and Dugdale, A. M., *Clerk and Lindsell on Torts* (2010, 20th Edition, London, Sweet & Maxwell)

Judge, S., *Business Law* (1999, 2th Edition, London, Macmillan Press)

Keenan, D., and Riches, S., *Business Law* (2007, 8th Edition, Edinburgh, Pearson Education)

Kellaway, E. A., *Principles of Legal Interpretation of Statutes, Contracts and Wills* (1995, Durban, Butterworths)

Kirk, D., '*Serious Fraud- A Banker's Perspective*', in Norton, J., *Banks Fraud and Crime* (1994, London, Lloyd's of London Press)

Kobsa, A., 'Privacy-Enhanced Web Personalization', in Brusilovsky, P., et al., *The Adaptive Web: Methods and Strategies of Web Personalization* (2007, Berlin, Springer Verlag)

Laidlaw, A., and Roberts, G., *Law Relating to Banking Services* (1992, 2nd Edition, London, Chartered Institute of Bankers)

Lambert, J., *Banking the Legal Environment* (1993, London, Routledge)

Lass, J. D., 'Fraud, Error and System Malfunction' in Goode, R., *Electronic Banking*: *The Legal Implications* (1985, Institute of Bankers and Centre for Commercial Law Studies, Queen Mary College, University of London)

Leigh, H. L., Banks-Fraud and Crime: A Survey of Criminal Offences under English Law*,* in Norton, J., (ed), *Banks: Fraud and Crime* (1994, London, Lloyd's of London Press)

Lewis, A., *Law of Banking Services: the Principles*, (1991, London, Eastham: Tudor)

Little, T., *Contract Law* (2012, Dundee, Dundee University Press)

Lowe, R., *Commercial Law* (1983, 6th Edition, London, Sweet & Maxwell)

Macleod, J., *Consumer Sales Law* (2002, 1st Edition, New York, Cavendish)

Mann, F. A., *The Legal Aspect of Money* (1992, 5th Edition, Oxford, Clarendon Press)

Markesinis, B. S., and Munday, R. J. C., *An Outline of the Law of Agency* (2005, 4th Edition, Oxford, Oxford University Press)

Marsh, S. B., and Soulsby, J., O*utlines of English Law* (1994, 5th Edition, London, McGraw-Hill)

Mason, S., *Electronic Banking: Protecting Your Rights* (2012, London, EMIS)

Mason, S., *Electronic Signatures in Law* (2003, London, LexisNexis)

Mavromati, D., *The Law of Payment Services in the EU* (2007, Netherlands, Kluwer Law International)

McBride, N., and Bagshaw, B., *Tort Law* (2008, 3rd Edition, London, Harlow Pearson Longman)

McGrath, P., *Commercial Fraud in Civil Practice* (2008, Oxford, Oxford University Press)

McGregor, H., *McGregor on Damages* (2009, 18th Edition, London, Sweet & Maxwell)

McKendrick, E., *Contract Law* (2010, 4th Edition, Oxford, Oxford University Press)

Michael, C., and Alistair, K., *Electronic Commerce, Law and Practice* (2002, 3rd Edition, London, Sweet & Maxwell)

Miles, R., *Blackstone's Sale and Supply of Goods and Services* (2001, London, Blackstone Press Limited)

Mitchell, C., et al., *Goff & Jones: The Law of Unjust Enrichment* (2011, 8th Edition, London, Sweet & Maxwell)

Norton, J., *Banks: Fraud and Crime* (1994, London, Lloyd's of London Press)

Peel, E., *The Law of Contract* (2007, 12th Edition, London, Sweet & Maxwell)

Pennington, R., et al., *Commercial Banking Law* (1978, 4th Edition, London, Macdonald & Evans)

Reed, C., *Internet Law*: *Text and Materials* (2004, 2nd Edition, Cambridge, Cambridge University Press)

Reynolds, B., *Boustead and Reynolds on Agency* (2001, 17th Edition, London, Sweet & Maxwell)

Riefa, C., and Hörnle, J., 'The Changing Face of Electronic Consumer Contracts in the Twenty-First Century: Fit for Purpose?', in Edwards, L., and Waelde, C., *Law and the Internet* (2009, 3rd Edition, Oxford, Hart)

Roberts, G., *Law Relating to Financial Services* (2009, 7th Edition, London, Global Professional Publishing)

Rosenthal, D., *Guide to Consumer Credit Law and Practice* (1994, London, Butterworths)

Ross, C., *Principles of Banking Law* (2002, 2nd Edition, Oxford, Oxford University Press)

Sadeghi, A. R., and Schneider, M., 'Electronic Payment Systems', in Becker, E., *Digital Rights Management* (2003, Germany, Springer-Verlag)

Saidov, D., and Cunnington, R., *Contract Damages* (2008, North America, Hart)

Salinger, J. D., *The Catcher in the Rye* (1994, London, Penguin)

Savage, N., and Bradgate, R., *Business Law* (1993, 2nd Edition, London, Butterworths)

Saxby, S., *Encyclopedia of Information Technology Law* (1990, loose-leaf, London, Sweet & Maxwell)

Sayer, P. E., *Credit Cards and the Law*: *An Introduction* (1988, London, Fourmat)

Schellekens, M., *Electronic Signatures: Authentication Technology from a Legal Perspective* (2004, Hague, T.M.C. Asser Press)

Sealy, L. S., and Hooley, J. A., *Commercial Law* (2009, 4th Edition, Oxford, Oxford University Press)

Sheldon, H. P., *The Practice and Law of Banking* (1958, 8th Edition, London, Macdonald & Evans)

Simpson, M., and Hoffmann, L., *Professional Negligence and Liability* (2012, 1st Edition, London, Informa)

Singlenton, S., *E-Commerce: A Practical Guide to the Law* (2003, Revised Edition, England, Gower)

Smart, E., 'Electronic Banking: An Overview of the Legal Implications', in Goode, R., *Electronic Banking*: *The Legal Implications* (1985, Institute of Bankers and Centre for Commercial Law Studies, Queen Mary College, University of London)

Smith, G. J. H., et al., *Internet Law and Regulation* (2007, London, Sweet & Maxwell)

Tapper, C., *Cross & Tapper on Evidence* (2007, 11th Edition, Oxford, Oxford University Press)

Todd, P., *Bills of Lading and Banker's Documentary Credits* (2007, 4th Edition, London, Informal)

Todd, P., *E-Commerce Law* (2005, London, Cavendish)

Toulson, R. G., and Phipps, C. M., *Confidentiality* (2006, 2nd Edition, London, Sweet & Maxwell)

Turner, J. E., *Money Laundering Prevention* (2011, New Jersey, John Wiley & Sons)

Tyree, A. L., and Beatty, A., *The Law of Payment Systems* (2000, Sydney, Butterworths)

Ulph, J., *Commercial Fraud: Civil Liability, Human Rights, and Money Laundering* (2006, Oxford, Oxford University Press)

Wadsley, J., and Penn, A. G., *The Law Relating to Domestic Banking* (2000, 2nd Edition, London, Sweet & Maxwell)

Walker, P., *Consumer Law* (2001, 4th Edition, London, Cavendish)

Wood, P. R., *Comparative Financial Law* (1995, London, Sweet & Maxwell)

Journal articles

Ahmad, N., 'E-commerce and legal issues surrounding credit cards: emerging issues and implications', (2009) 15 *Computer and Telecommunications Law Review* 114-123

Ahmad, N., 'Internet intermediary liability: a comparative overview', (2011) 17 (4) *Computer and Telecommunications Law Review* 108-113

Akindemowo, E., 'Contract, deposit or e-value? reconsidering stored value products for a modernized payments framework', (2009) 7 *DePaul Business & Commercial Law Journal* 275-336

Akintoye, K. A., and Araoye, O. I., 'Combating e-fraud on electronic payment system', (2011) 25 *International Journal of Computer Applications* 48-53

Alhosani, W., 'Banking confidentiality versus disclosure', (2012) *Durham Law Review* 1-19

Ali Khan, L., 'A theoretical analysis of payment systems', (2008) 60 *South Carolina Law Review* 425-489

Alqudah, F., 'Banks' duty of confidentiality in the wake of computerised banking', (1995) 10 *International Banking Law* 50-55

Angel, J., 'Why use digital signatures for electronic commerce?', (1999) 2 *Journal of Information, Law and Technology*

http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_2/angel/ [23 February 2011]

Anning, P., 'Payment Services Directive: a detailed proposal by the European Commission for a new legal framework', (2006) 21 *International Banking Law and Regulation* 344-353

Arora, A., 'Banking regulation of UK and US financial markets', (2008) 9 *Banking Regulation* 224

Arora, A., 'Contractual and tortious liability in EFT transactions in the United Kingdom', (1992) 1 (3) *Law, Computers & Artificial Intelligence* 291-309

Arora, A., 'Truncation of cheque and other instruments through EFT: Part 1', (1994) 13 *International Banking and Financial Law* 48-51

Arora, A., 'Unfair contract terms and unauthorised bank charges: a banking lawyer's perspective', (2012) *Journal of Business Law* 44-70

Azzouni, A., 'Internet banking and the law: a critical examination of the legal controls over internet banking in the UK and their ability to frame, regulate and secure banking on the net', (2003) 18 (9) *International Banking Law and Regulation* 351-362

Balboni, P., 'Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication', (2004) 13 *Information & Communications Technology Law* 211-242

Barker, K. J., et al., 'Credit card fraud: awareness and prevention', (2008) 15 *Journal of Financial Crime* 398-410

Bergsten, E. E., 'Legal aspects of international Electronic Funds Transfers', (1987) 7 *International Business Law* 649-668

Bohm, N., and Brown, I., 'Electronic commerce: who carries the risk of fraud?', (2000) *Journal of Information, Law and Technology* 1-42

Bollen, R., ‘A discussion of best practice in the regulation of payment services: part 1’, (2010) 25 *International Banking Law and Regulation* 370-380

Bollen, R., ‘A discussion of best practice in the regulation of payment services: part 2’, (2010) 25 *International Banking Law and Regulation* 429-440

Bollen, R., ‘A review of the development and legal nature of payment facilities’ (2005) 16 *Journal of Business and Law* 93-127

Bollen, R., ‘European regulation of payment services – recent developments and proposed Payment Services Directive – Part 2’, (2007) 22 (10) *International Banking Law and Regulation* 532-548

Bollen, R., ‘European regulation of payment services – the story so far’, (2007) 22 (9) *International Banking Law and Regulation* 451-468

Bollen, R., ‘Harmonisation of international payment law: a survey of the UNCITRAL model law on credit transfers: Part 1’, (2008) 23 (2) *International Banking Law and Regulation* 44-63

Bollen, R., ‘Harmonisation of international payment law: a survey of the UNCITRAL model law on credit transfers: Part 2’, (2008) 23 (3) *International Banking Law and Regulation* 105-124

Bollen, R., ‘Setting international regulatory standards for hedge funds: Part 1’, (2011) 26 *International Banking Law and Regulation* 59-71

Bollen, R., ‘Setting international regulatory standards for hedge funds: Part 2’, (2011) 26 *International Banking Law and Regulation* 105-118

Bollen, R., ‘Setting international regulatory standards for hedge funds: Part 3’, (2011) 26 *International Banking Law and Regulation* 174-187

Bollen, R., ‘What a payment is and how it continues to confuse lawyers’, (2005) 12 *E-Law- Murdoch University Electronic Journal of Law* 1-13

Bond, M., et al., 'Chip and Skim: cloning EMV cards with the pre-play attack', (2012) *arXiv preprint arXiv: 1209.2531* 1-21 http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf [15 March 2013]

Booysen, S. A., 'Bank secrecy in Singapore and the customer's consent to disclosure', (2011) 26 *Journal of International Law and Regulation* 501-508

Boss, A. H., 'Convergence in electronic banking: technological convergence, systems convergence, legal convergence', (2009) 2 *Drexel Law Review* 63-103

Brandt, P., and Graham, P., 'An update on the UK's implementation of the Payment Services Directive', (2009) 64 *Compliance Officer Bulletin* 1-35

Caminer, B. F., 'Credit card fraud: the neglected crime', (1985) 76 *Criminal Law & Criminology* 746-763

Caskey, J. P. and Sellon, G. H., 'Is the debit card revolution finally here?', (1994) 4 *Economic Review* 79-95

Chandler, J. A., 'Negligence liability for breaches of data security', (2008) 23 *Banking and Finance Law Review* 223-274

Chang, J. S., and Chong, M. D., 'Psychological influences in e-mail fraud', (2010) 17 *Journal of Financial Crime* 337-350

Chris, R., 'What is a signature?', (2000) 3 *Journal of Information, Law and Technology* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed [20 February 2011]

Chung, C. S., and Byer, D. J., 'The electronic paper trail: evidentiary obstacles to discovery and admission of electronic evidence', (1998) 22 *Journal of Science & Technology Law* 1-21

Coleton, A., 'Banking insolvency regimes and cross-border banks – complexities and conflicts: is the current European insolvency

framework efficient and robust enough to effectively resolve cross-border banks, can there be a one size fits all solution?', (2012) 27 (2) *International Banking Law and Regulation* 63-81

Collingwood, L., 'Privacy in Cyberworld: Why lock the gate after the horse has bolted?', (2012) 3 (1) *European Journal of Law and Technology* 1-11 http://ejlt.org//article/view/110/189

Collins, V., 'Computerised evidence: finding the right approach', (1994) 3 *Nottingham Law Journal* 11-33

Connearn, P., 'Credit reference agencies and the credit report: Part 1', (2012) 26 *Quarterly Account, Money Advice Association* 28-29

Cornelius, S., 'The legal nature of payment by credit card', (2003) 15 *Mercantile Law Journal* 153-171

Davies, B., 'What is the extent of the customer's duty not to facilitate fraud?', (2009) 30 (11) *Business Law Review* 238-242

Dickens, R. L., 'Finding common ground in the world of electronic contracts: the consistency of legal reasoning in clickwrap cases', (2007) 11 *Marquette Intellectual Property Law Review* 379-412

Dolan, J. F., 'Impersonating the drawer: a comment on professor Geva's consumer liability in unauthorized Electronic Funds Transfers', (2003) 38 *Canadian Business Law Journal* 282-293

Douglass, D. B., 'An examination of the fraud liability shift in consumer card-based payment systems', (2009) 33 *Journal of Economic Perspectives* 43-49

Dow, S. B., 'Damages under the Federal Electronic Funds Transfer Act: a proposed construction of sections 910 and 915', (1985) 23 *American Business Law Journal* 1-83

Edwards, R., ‘Fraud loss under the Australian Electronic Funds Transfer Code: is it efficient?’, (2009) 24 *International Banking Law and Regulation* 361-367

Eisenschitz, T., ‘E-mail law’, (2002) 54 *Aslib Proceedings* 41-47

England, C., ‘Are banks special?’, (1991) 14 *Regulation* 25-34

Facciolo, F., ‘Unauthorized payment transactions and who should bear the losses’, (2008) 83 *Chicago-Kent Law Review* 605-631

Farrand, J., and Clarke, A., ‘Observations’, (2012) 62 *Emmet and Farrand on Title Bulletin* 1-5

Ferretti, F., ‘Consumer credit information system: a critical review of the literature too little attention paid by lawyers?’, (2007) 23 *European Journal of Law and Economics* 71-88

Ferretti, F., ‘Re-thinking the regulatory environment of credit reporting: could legislation stem privacy and discrimination concerns?’, (2006) 14 (3) *Journal of Financial Regulation and Compliance* 254-272

Finch, V., ‘Security, insolvency and risk: who pays the price?’, (1999) 62 (5) *The Modern Law Review* 633-670

Fisher, J., ‘The UK’s faster payment project: avoiding a bonanza for cybercrime fraudsters’, (2008) 15 *Journal of Financial Crime* 155-164

Fletcher, N., ‘Challenges for regulating financial fraud in cyberspace’, (2007) 14 *Journal of Financial Crime* 190-207

Fofaria, A., ‘Excluding the recovery of “consequential and indirect losses” in English and French laws’, (2006) 5 *International Business Law* 597-615

Ford, M. D., ‘Identity authentication and e-commerce’, (1998) 3 *Journal of Information, Law and Technology*

http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/ford [20 April 2011]

Geva, B., 'Consumer liability in unauthorized Electronic Funds Transfers', (2003) 38 *Canadian Business Law Journal* 207-281

Geva, B., 'Payment finality and discharge in funds transfers', (2008) 83 *Chicago-Kent Law Review* 633-677

Geva, B., 'Payment into a bank account', (1990) 5 *International Banking Law* 108-118

Geva, B., 'Payment transactions under the EU Payment Services Directive: a U.S. comparative perspective', (2009) 27 *Penn State International Law Review* 713-755

Geva, B., 'Recent international development in the law of negotiable instruments and payment and settlement systems', (2007) 42 *Texas International Law Journal* 685-726

Geva, B., 'The concept of payment mechanism', (1986) 24 *Osgoode Hall Law oJournal* 1-34

Geva, B., 'The E.F.T. debit card', (1989) 15 *Canadian Business Law Journal* 406-440

Gillette, C. P., and Walt, S., 'Uniformity and diversity in payment systems', (2008) 83 *Chicago-Kent Law Review* 499-559

Gonzalez, A., 'PayPal: the legal status of C2C payment systems', (2004) 20 (4) *Computer Law & Security Report* 293-299

Goode, R., 'The banker's duty of confidentiality', (1989) *Journal of Business Law* 269-272

Halladay, M. J., 'Remoteness of contractual damages', (2009) 21 *The Denning Law Journal* 173-179

Hannan, T. H., and Hanweck, G. A., 'Bank insolvency risk and the market for large certificates of deposit', (1988) 20 *Journal of Money, Credit and Banking* 203-211

Harris, S. L., 'Introduction to rethinking payments law', (2009) 83 *Chicago-Kent Law Review* 477-484

Hart, O. D. and Jaffee, D. M., 'On the application of portfolio theory to depository financial intermediaries', (1974) 41 *The Review of Economic Studies* 129-147

Haynes, A., 'Financial promotions – rules and principles', (2008) 29 (3) *Company Lawyer* 89-90

Haynes, A., 'Market abuse, fraud and misleading communications', (2012) 19 (3) *Journal of Financial Crime* 234-254

Haynes, A., 'Misleading communications – the unnoticed danger', (2010) 31 (8) *Company Lawyer* 229-230

Haynes, A., 'Money laundering: from failure to absurdity', (2008) 11 (4) *Journal of Money Laundering Control* 303-319

Haynes, A., 'Where there's muck there's brass – virtual exchanges and future equity finance', (2009) 30 (9) *Company Lawyer* 257-258

Heller, S., 'A proposal for consideration of a unified payments law', (2009) 83 *Chicago-Kent Law Review* 485-497

Hogg, M., 'Secrecy and signatures-turning the legal spotlight on encryption and electronic signatures', (2000) *AHRC Research Centre for Studies in Intellectual Property and Technology Law* 1-13

Hood, P., 'Remoteness of damage in contract revisited', (1996) 1 *Edinburgh Law Review* 127-135

Hooley, R., ‘‘Bankers’ references and the bank’s duty of confidentiality: when practice does not make perfect’, (2000) 59 *The Cambridge Law Journal* 21-23

Hornle, J., ‘The European Union takes initiative in the field of e-commerce’, (2000) 3 Journal of Information Law & Technology http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/hornle [31 May 2013]

Howells, G., ‘Data protection, confidentiality, unfair contract terms, consumer protection and credit reference agencies’, (1995) *Journal of Business Law* 343-359

Hughes, S. J., ‘Policing money laundering through funds transfers: a critique of regulation under the Bank Secrecy Act’, (1992) 67 *Indiana Law Journal* 283-330

James, E., et al., ‘Proposed model rules governing the admissibility of computer-generated evidence’, (1999) 15 *Santa Clara Computer & High Technology Law Journal* 1-73

Jiang, S., and Gong, G., ‘Password based key exchange with mutual authentication’, (2005) 3357 *Lecture Notes in Computer Science* 267-279

John, A., and Guadamuz, A., ‘Electronic money: the European regulatory approach’, (2008) The *New Legal Framework for E-Commerce in Europe* 173-201

Joris, C., et al., ‘On the security of today’s on-line electronic banking systems’, (2002) 11 http://www.linkedin.com/in/jorisc/pub/stoebs.pdf [21 February 2013]

Joris, T., and Gutwirth, S., ‘Electronic funds transfer and the consumer: the “soft law” approach in the European Community and Australia’, (1991) 40 (2) *International & Comparative Law Quarterly* 265-301

Kaminski, C., ‘Online peer-to-peer payments: PayPal primes the pump, will banks follow?’, (2003) 7 *North Carolina Banking Institute* 375-404

Kethi K., ‘An analysis of the legal challenges posed by electronic banking’, (2007) 1 *Kenya Law Review* 323-341

Kilonzo, K. D., ‘An analysis of the legal challenges posed by electronic banking’, (2007) 1 *Kenya Law Review* 323-341

King, R., ‘The receiving bank’s role in credit transfer transactions’, (1982) 45 *Modern Law Review* 369-383

Koh, P., ‘Some issues in misrepresentation’, (2008) 2 *Journal of Business Law* 123-138

Kolodziej, A., ‘Customer-banker liability in electronic banking’, (1986) 7 *Company Lawyer* 191-194

Koutsias, M., ‘Privacy and data protection in an information society: how reconciled are the English with the European union privacy norms?’, (2012) 18 (8) *Computer and Telecommunications Law Review* 261-270

Kraakman, H., ‘Corporate liability strategies and the costs of legal controls’, (1984) 93 *Yale Law Journal* 857-895

Kraakman, H., ‘Gatekeepers: the anatomy of a third-party enforcement strategy’, (1986) 2 *Journal of Law, Economics & Organization* 53-75

Kull, A., ‘Restitution and final payment’, (2008) 83 (2) *Chicago-Kent Law Review* 677-687

Landey, K. M., ‘Consumer-cardholder defenses in tripartite credit card arrangements: a battleground for the beleaguered bank’, (1983) 88 *Commercial Law Journal* 84-98

Lanskoy, S., ‘The legal nature of electronic money’, (2000) 73 *Banque de France Bulletin* 21-49

Levi, M., and Burrows, J., ‘Measuring the impact of fraud in the UK: a conceptual and empirical journey’, (2008) 48 *British Journal of Criminology* 293-318

Levitin, A. J., ‘Private disordering: payment card fraud liability rules’, (2011) 5 *Brooklyn Journal of Corporate, Finance and Commercial Law* 1-48

Levitin, A. J., ‘The merchant-bank struggle for control of payment system’, (2006) 17 *Journal of Financial Transformation* 73-84

Liao E., et al., ‘A password authentication scheme over insecure network’, (2006) 72 *Journal of Computer and System Sciences* 727-740

Lin Yu, H., ‘Duty of confidentiality: myth and reality’, (2012) 31 *Civil Justice Quarterly* 68-88

Lista, A., ‘Card payment system and competition concerns: multilateral interchange fees and no-discrimination rules, a necessary evil?’, (2008) 7 *Journal of Business Law* 688-715

Lucia, J. S. S., ‘Exchange losses from international Electronic Funds Transfers: time to unify the law’, (1988) 8 *Northwestern Journal of International Law & Business* 759-787

Luedtke, S. M., and Gross, J. D., ‘Electronic Fund Transfers: regulation and the right to financial privacy’, (1981) 16 *Gonzaga Law Review* 313-355

Mackenzie, R., ‘Virtual money laundering, vanishing law: dematerialisation in electronic funds transfer, financial wrongs and doctrinal makeshifts in English legal structures’, (1998) 2 *Journal of Money Laundering Control* 22-32

Maduegbuna, S. O., ‘The effects of electronic banking techniques on the use of paper-based payment mechanism in international trade’, (1994) *Journal of Business Law* 388-362

Mann, F. A., ’Recovering currency exchange losses’, (1988) 104 *Law Quarterly Review* 3-6

Mann, R. J., 'Credit cards and debit cards in the United States and Japan', (2002) 20 *Monetary and Economic Studies* 123-162

Mann, R. J., 'Regulating internet payment intermediaries', (2004) 82 *Texas Law Review* 681-716

Marks, N. A., 'The evolution of retailer, banker and customer relationships: a conceptual framework', (1998) 26 (6) *International Journal of Retail & Distribution Management* 225-236

Marten, R., 'The customer's duty to take care in the exercise of an account: a criticism of Tai Hing Cotton Mills v. Liu Chong Hing Bank Ltd', (1986) 2 *Professional negligence* 17-19

Mason, S., 'Electronic signatures in practice', (2006) VI *Journal of High Technology Law* 148-164

Mason, S., and Bromby, M., 'Response to digital agenda for Europe: electronic identification, authentication and signatures in the European digital single market: Public consultation', (2012) 3 *European Journal of Law and Technology* 1-9

Mayes, D. G., 'Who pays for bank insolvency?', (2004) 23 *Journal of International money and Finance* 515-551

McAndrews, J. J., 'E-money and payment system risks', (1999) 17 *Contemporary Economic Policy* 348-357

McBryde, W., 'Remedies for breach of contract', (1996) 1 *Edinburgh Law Review* 43-78

McKnight, A., 'A review of developments in English law during 2005: part 1', (2006) 21 (3) *International Banking Law and Regulation* 117-148

McMeel, G., 'Conduct of banking business brought into the FSA fold', (2011) *Lloyd's Maritime and Commercial Law Quarterly* 431-452

McMeel, G., 'Contract damages: the interplay of remoteness and loss of a chance', (2004) 1 *Lloyd's Maritime and Commercial Law Quarterly* 10-14

Mroz, D. M., 'Credit or debit? Unauthorized use and consumer liability under federal consumer protection legislation', (1999) 19 *Northern Illinois University Law Review* 589-628

Mthembu, M. A., 'Electronic Funds Transfer: exploring the difficulties of security', (2010) 5 (4) *Journal of International Commercial Law and Technology* 201-205

Murray, J., 'Public key infrastructure digital signatures and systematic risk', (2003) *Journal of Information, Law and Technology* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/murray/?textOnly=false [7 March 2012]

Nam, J., et al., 'Security weakness in a three-party pairing-based protocol for password authenticated key exchange', (2007) 177 *Information Sciences* 1364-1375

Newman, S., and Sutter, G., 'Electronic payments- the smart card', (2002) 18 (4) *Computer Law & Security Report* 235-240

Nolan, R., Publication Review, 'Restitution and banking law', (1999) 115 *Law Quarterly Review* 688-693

O'Connor, M., and Brownsdon, E., 'Electronic signatures', (2002) 152 (7022) *New Law Journal* 348-351

O'Reilly, C., 'Finding jurisdiction to regulate Google and the Internet', (2011) 2 *European Journal of Law and Technology* 1-13

Odry, G., 'Exclusion of consequential damages: write what you mean', (2012) 29 (2) *The International Construction Law Review* 142-164

Ogilvie, M. H., 'From secrecy to confidence to the demise of the banker customer relationship: *Rodaro v. Royal Bank of Canada*', (2003) 19 *Banking and Financial Law Review* 103-116

Ogivie, M. H., ‘Banker and customer: the five-year review 2000-2005’, (2007) 23 *Banking and Finance Law Review* 107-164

Oliver, D. J., ‘Plastic card fraud: a matter of intelligence’, (1995) 2 *Journal of Financial Crime* 300-305

Ormerod, D., ‘The Fraud Act 2006 - criminalising lying’, (2007) *Criminology Law Review* 193-219

Pavia, J. M., et al., ‘Credit card incidents and control systems’, (2012) *International Journal of Information Management* 1-3

Pelly, L. S., ‘Bradley Crawford, payment, clearing and settlement in Canada’, (2004) 40 *Canadian Business Law Journal* 466-474

Porter, D., ‘Insider fraud: spotting the wolf in sheep's clothing’, (2003) 4 *Computer Fraud and Security* 12-15

Pruitt, D. N., ‘Beyond fair use: the right to contract around copyright protection of reverse engineering in the software industry’, (2006) 6 *Chicago-Kent Journal of Intellectual Property* 66-86

Putland, P. A., et al., ‘Electronic payment systems’, (1997) 15 (2) *BT Technology Journal* 32-38

Rahmatian, A., ‘Must cheques disappear by 1018?’, (2011) 26 *International Banking Law and Regulation* 310-312

Rai, A. K., ‘Electronic customer relationship management: a tool for sustained success in services organisations’, (2011) 1 *Asian Journal of Technology & Management Research* 1-10

Ramage, S., ‘Digital money, electronic fraud, new regulations and the old money laundering regulations’, (2011) 200 *Journal of Criminal Lawyer* 1-3

Rawlings, P., ‘Avoiding the obligation to lend’, (2012) 2 *Journal of Business Law* 89-110

Reed, C., 'Consumer electronic banking', (1994) 9 (11) *International Banking Law* 451-463

Richard, G. and Kunkwl, J. D., 'Recent development in shrinkwrap, clickwrap and browsewarp licenses in the United States', (2002) 9 (3) *Murdoch University Electronic Journal of Law* 1-18

Riefa, C., '"To be or not to be an auctioneer?" some thoughts on the legal nature of online "eBay" auctions and the protection of consumers', (2008) *Journal of Consumer Policy* 67-108

Riefa, C., 'The reform of electronic consumer contracts in Europe: towards an effective legal framework?', (2009) 14 *Lex Electronica* 1-44

Riem, A., 'To catch a cyber thief: tracing internet crime', (2007) 184 *The In-House Layer* 43-47

Robertson, A., 'The basis of the remoteness rule in contract', (2008) 28 (2) *Legal Studies* 172-196

Rochet, J. C., and Tirole, J., 'Controlling risk in payment systems', (1996) *28 Journal of Money, Credit and Banking* 832-862

Rogers, J. S, 'The new old law of electronic money', (2005) 58 *Social Science Research Network* 1253-1311

Rogers, J. S., 'The basic principle of loss allocation for unauthorized checks', (2004) 39 *Wake Forest Law Review* 453-509

Rogers, J. S., 'The irrelevance of negotiable instruments concepts in the law of the check-based payment system', (1987) 65 *Texas Law Review* 929-961

Rogers, J. S., 'Unification of payments law and the problem of insolvency risk in payment systems', (2008) 83 *Chicago Kent Law Review* 689-720

Rosenberg, A. S., 'Better than cash? global proliferation of payment cards and consumer protection policy', (2006) 60 *Consumer Finance Law Quarterly Report* 426-459

Rusch, L. J., 'Reimagining payment systems: allocation of risk for unauthorized payment inception', (2008) 83 *Chicago-Kent Law Review* 561-605

Sappideen, R., 'Cross-border Electronic Funds Transfers through large value transfer system, and the persistence of risk', (2003) 13 *Journal of Business Law* 584-602

Schulze, W., 'Smart cards and e-money: new developments bring new problems', (2004) 16 *South Africa Mercantile Law Journal* 703-715

Sealy, L. S., 'The Settlement Finality Directive – points in issue', (2000) 2 *Company Financial and Insolvency Law Review* 221-228

Seyad, S. M., 'A critical assessment of the Payment Service Directive', (2008) 23 (4) *International Banking Law and Regulation* 218-230

Shinn, E. T., 'An overview of unauthorized Electronic Funds Transfers: alternatives in reducing consumer liability', (1985) 90 *Commercial Law Journal* 216-221

Shy, O., and Tarkka, J., 'The market for electronic cash cards', (2002) 34 (2) *Journal of Money, Credit & Banking* 299-314

Simon, S. M., and Victor, T. F., 'Customers' risk perceptions of electronic payment systems', (1994) 12 (8) *International Journal of Bank Marketing* 26-38

Singh, D., 'The UK Banking Act 2009, per-insolvency and early intervention: policy and practice', (2011) *Journal of Business Law* 20-42

Skajaa, L., 'International Hull Clauses 2002: a contractual solution to the uncertainty of the fraudulent claims rule?', (2003) Part 2 *Lloyd's Maritime and Commercial Law Quarterly* 279-288

Sorkin, D. E., 'Payment methods for consumer-to-consumer online transaction', (2001) 35 *Akron Law Review* 1-30

Spearman, R., 'Disclosure of confidential information: *Tournier* and ''disclosure in the interests of the bank'' reappraised', (2012) *Journal of International Banking and Financial Law* 78-82

Spyrelli, C., 'Electronic signatures: a transatlantic bridge? an EU and US legal approach towards electronic authentication', (2002) 2 *Journal of Information, Law and Technology* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/ [23 February 2011]

Stem, A., 'Judgments in foreign currencies: a comparative analysis', (1997) *Journal of Business Law* 266-288

Stokes, R., 'The banker's duty of confidentiality, money laundering and the Human Rights Act', (2007) *Journal of Business Law* 502-526

Stokes, R., 'The genesis of banking confidentiality', (2011) 32 (3) *The Journal of Legal History* 279-294

Sullivan, R. J. and Wang, Z., 'Nonbanks in the payment system: innovation, competition, and risk, a conference summary', (2007) 3 *Economic Review Journal* 83-106

Tan, Y. H., and Thoen, W., 'Toward a generic model of trust for electronic commerce', (2001) 5 (2) *International Journal of Electronic Commerce* 61-74

Tapper, C., 'Evidence and computers', (1984) 101 *South African Law Review* 675-690

Tettenborn, A., 'Consequential damages in contract-the poor relation?', (2008) 42 *Loyola of Los Angeles Law Review* 177-195

Thevenoz, L., 'Error and fraud in wholesale funds transfers: U.C.C. Article 4A and The UNCITRAL harmonization process', (1991) 42 (2) *Alabama Law Review* 881-949

Thomas, S. B., 'Electronic Funds Transfer and fiduciary fraud', (2005) *Journal of Business Law* 48-69

Thompson, A. C., 'The legal relationship between banker and customer: the duty of secret', (1926) 43 *The South African Law Journal* 9-18

Tommie, S., and Steven, U.J., 'Guard against cybertheft', (2010) 210 (4) *Journal of Accountancy* 42-49

Turner, M., 'Is shopping online now risk free for UK consumers?', (2006) 22 *Computer Law and Security Report* 333-337

Walden, I., 'Data security and document image processing: legal security of cross-border electronic banking', (1994) 9 *International Banking Law* 506-518

Wang, M., 'Do the regulations on electronic signatures facilitate international electronic commerce? a critical review', (2007) 23 *Computer Law & Security Report* 32-41

Woodruff, B. E., 'Electronic Funds Transfer in the bank card industry', (1977) 501 (3) *Washington University Law Quarterly* 501-506

Worthington, S., 'The card centric distribution of financial services: a comparison of Japan and the UK', (1998) 16 (5) *International Journal of Bank Marketing* 221-220

Yao, Y., 'A legal snapshot of the lead bank: the position and responsibilities in arranging a syndicated loan', (2010) 25 (3) *International Banking Law and Regulation* 148-152

Zentner, J., and Peckham, A., 'The new EFT code of conduct', (2001) 16 *International Banking Law* 242-245

Zubair, M., and Ali, A., ‘An analysis of duty of confidentiality owed by banker to its customers’, (2009) *Social Science Research Network* 1-14

Official documents and government publications

Department for Business, Innovation and Skills, *Draft Consumer Rights Bill* (2013, London, BIS/13/925, Cm 8657) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206367/bis-19-925-draft-consumer-rights-bill.pdf [03 September 2013]

General Secretariat of the Council of the EU, *Commission Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market* (2004, Brussels, COD, 920) http://ec.europa.eu/internal_market/services/docs/services-dir/notes/explan-note-healthcare_en.pdf [20 March 2011]

House of Lords, Science and Technology Committee, *Personal Internet Security: Follow-up* (2008, 4th Report, London, the Stationary Office Limited) http://www.publications.parliament.uk/pa/ld200708/ldselect/ldsctech/131/131.pdf [20 May 2012]

Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions - Advice from the Law Commission*, December 2001, http://lawcommission.justice.gov.uk/docs/Electronic_Commerce_Advice_Paper.pdf [14 July 2011]

Office of Fair Trading, *UK payment systems: An OFT market study of clearing systems and review of plastic card networks* (May 2003) http://www.oft.gov.uk/shared_oft/reports/financial_products/oft658.pdf [14 July 2013]

Report by the Review Committee on Banking Services: Law and Practice, ("The Jack Report") (1989, London, HMSO, Cm 622)

UK Government, *Banking Services: Law and Practice* (1990, London, HMSO, Cm

Media and Internet sources

Bank for International Settlements, 'Payment systems in the United Kingdom', in *The Red Book* (2003) http://www.bis.org/publ/cpss53p14uk.pdf [17 July 2013]

Barclays, *Terms and conditions* http://www.barclays.co.uk/ImportantInformation/TermsandConditions/P1242575350746 [20 April 2013]

European Payment Council website http://www.europeanpaymentscouncil.eu [5 July 2013]

Experian, *The Credit Reference Agency Explained, A Guide for Consumer Advisers*, (2013) http://www.experian.co.uk/downloads/consumer/creditRefAgencyExplained.pdf [3 February 2013]

HSBC, *General terms and conditions*, http://www.hsbc.co.uk/content_static/en/ukpersonal/pdfs/en/personalbankingterms_conditions.pdf [20 April 2013]

Lloyds TSB, *Your banking relationship with us,* http://www.lloydstsb.com/assets/media/pdfs/banking_with_us/personal_banking_terms_and_conditions.pdf [20 April 2013]

The Lending Code 2012, http://boini.bankofireland.com/fs/doc/wysiwyg/lendingcode.pdf [5 March 2013]

Tyree, A.L., 'Payment by Credit Card', (2009) http://www.austlii.edu.au/~alan/payment-by-credit-card.html.24sep2009 [20 December 2010]

UK Payments Administration, *CHAPS Facts and Figures* (2010) http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/chaps_facts_and_figures/ [20 February 2011]

UKCards Association, *Annual Report 2013*, http://www.theukcardsassociation.org.uk/wm_documents/Final%20AR_2012_interactive_sml.pdf [14 July 2013]

UNCITRAL website http://www.uncitral.org/uncitral/en/index.html [15 July 2013]

Dissertations

Chen, Z., *Electronic Payment Systems: General Review and Comparative Analysis* (2004) Thesis (Master) University of Texas

Longe, O., Consumers, *Electronic Funds and the Law: The Inadequate Protection of Consumer EFT Users in England Evaluated Against the American Experience*, (1992) Thesis (PhD) University of London

Louw, M. K., *Selective Legal Aspects of Bank Demand Guarantees* (2008) Thesis (PhD) University of South Africa

Semmens, N., *The Fear of Plastic Card Fraud* (2002) Thesis (PhD) University of Sheffield

Walton, P., *Priority Rights of Creditors in Insolvency* (2003) Thesis (PhD) University of Wolverhampton

White, P., *The Regulation of Electronic Funds Transfer in Australia: An Integrated Multidisciplinary Approach* (2007) Thesis (PhD) Victoria University

Conference papers

Chen, H., and Corriveau, J. P., *Security testing and compliance for online banking in real-world*, The International Multi Conference of Engineers and Computer Scientists (2009), Hong Kong

González, A. G., *PayPal and eBay: the legal implications of the C2C electronic commerce model,* BILETA Conference (2009), London

Kempson, E., *Looking beyond our shores: consumer protection regulation lessons from the UK*, Joint Center for Housing Studies (2008), Harvard University

Li, W., *Finality rules within the law of domestic large value Renminbi Electronic Funds Transfers (EFT) in China,* BILET Conference (2007), Hertfordshire

Mayes, D. G., *The role of the safety net in resolving large financial institutions,* Federal Reserve Bank of Chicago Conference (2004), Chicago

Prior, F., and Santoma, J., *The use of prepaid cards for banking the poor*, IESE Conference (2008), University of Navarra

Smith, R. G., and Grabosky, P., *Plastic card fraud, Australian Institute of Criminology* Conference (1998), Melbourne

Turner, C. W., et al., *Factors that affect the perception of security and privacy of e-commerce web,* International Conference on Electronic Commerce Research (2001), Dallas

Weiner, W., and et al., *Nonbanks and risk in retail payments,* Joint Bank of England/European Central Bank Conference (2007), Frankfurt