

E-commerce Protocol Supporting Automated Online Dispute Resolution

Saleh Ibrahim Alfuraih

Ph.D. Thesis

**School of Computing Science
University of Newcastle upon Tyne**

September 2005

NEWCASTLE UNIVERSITY LIBRARY

204 26683 5

Thesis L8092

Abstract

E-commerce now constitutes a significant part of all commercial activity; however the increase in transactions is also leading to more disputes. These disputes are becoming more frequent, more technologically complicated and more difficult in terms of traceability.

This thesis focuses specifically on dispute problems related to soft products, i.e. those that are intangible and therefore requiring no physical delivery. With the growing demand for these types of products, e.g. downloadable films, music, software, and prepaid calling time, the prevention of fraudulent transactions is becoming increasingly important. Reasons for the rise in the number of fraudulent transactions include merchants being unable to see the customer to verify an ID or signature and E-commerce enabling soft-products and services to be acquired via soft delivery methods: email, download or logging in.

The introductory section provides a critique of current e-commerce fraud detection and prevention techniques and shows that not all are suitable for e-commerce, especially soft-products, and therefore unable to provide complete protection against fraud. The future relating to the detection and prevention of e-commerce fraud is then discussed, leading to suggestions regarding the improvement of the current state-of-the-art technique, the Address Verification Service (AVS), which is used to accommodate the introduction of soft-products.

Apart from the exchange process problems, i.e. those involving money and goods, attention is also paid to other important factors such as timing and quality that are usually neglected in these detection and prevention techniques. Dispute scenarios from many different perspectives have been analysed, viz. computer science, business, legal and that of the participants themselves. From the analyses, all possible dispute cases have been formally listed using the 'Truth Table' approach. This analysis has then led to the design of a comprehensive taxonomy framework for dispute in e-commerce.

The term Online Dispute Resolution (ODR), is the online technology applied to Alternative Dispute Resolution (ADR) which is resolving disputes other than via litigation in the courts. Current ODR systems and their suitability for the e-commercial world have been examined, concluding that not all are appropriate for e-commerce situations (since most still involve a human element and often make the resolution process more costly than the actual item under dispute).

The proposed solution to the problem is by automating the online dispute resolution process. The total solution is described in two parts (i) an E-commerce Transaction Protocol (ETP) forming the infrastructure where the transaction will take place and be able to accommodate any new improvements in the future, and (ii) an Automated Online Dispute Resolution (AODR) system which should automatically resolve any dispute occurring within the proposed e-commerce model. In order for the AODR to resolve any dispute, a product/payment specific plug-in (add-on) has been incorporated into the system. For illustration purposes, credit cards as a payment method has been selected and the appropriate plug-in specification for soft products and credit cards created.

The concept of providing every soft product with a quality certificate has also been discussed. A concluding case study of e-commerce in Saudi Arabia has been used to test the viability of both the e-commerce dispute taxonomy and the proposed model. The case study shows the suitability of using ETP with AODR in order to resolve soft-product disputes automatically. Limitations of the work and further research possibilities have then been identified.

Acknowledgements

My first and foremost thanks go to my God then to my supervisor Dr Richard Snow for his guidance, encouragement and support throughout my PhD study at Newcastle University. His style of supervision has granted me so much space to expand my thoughts and exploit new areas. He reviewed the drafts of this thesis carefully and provided lots of important suggestions for improvement; I greatly appreciate his excellent supervision with time and effort.

I am very grateful to my thesis committee for their invaluable advice and insightful comments. Thanks to the Department of Computing Science for its support during my Ph.D. programme. The Department has been extremely helpful in financing me to attend conferences which have been an important and exciting element of my research. Thanks to all the personnel of the department for creating an inspiring and comfortable research atmosphere. All my friends at college have made the past few years very enjoyable.

Final thanks go to my parents, my wife and my daughters for their understanding and encouragement which helped me through many tough times.

TABLE OF CONTENTS

1.	Introduction	1
1.1	Electronic Commerce	2
1.2	E-commerce Products.....	2
1.3	E-commerce Fraud and Fraud Prevention.....	3
1.4	Fair Exchange and Non-Repudiation	4
1.5	Example Scenario.....	5
1.6	Scope	6
1.7	The Proposed Solution	6
1.8	Structure of the Thesis.....	7
2	Electronic Commerce and Payments	10
2.1	Introduction	11
2.2	E-Commerce Definition	12
2.3	History of E-commerce	13
2.4	E-commerce Products.....	13
2.5	Categories of E-commerce	16
2.6	Future of E-commerce.....	19
2.7	E-commerce Security	20
2.8	Trust in E-commerce	20
2.9	Payments Methods.....	21
2.9.1	Payment Characteristics	21
2.9.2	Contradictions of Characteristics	24
2.9.3	Traditional Payment Methods	27
2.9.3.1	Cash	27
2.9.3.2	Cheques	29
2.9.3.3	Credit Cards.....	32
2.10	E-Payment Methods	37
2.10.1	Payment Cards.....	37
2.10.2	E-Direct Debit	38
2.10.3	Electronic and Mobile Banking.....	39
2.10.4	Centralized Account Systems.....	41
2.10.5	Telephony Account Systems	42
2.10.6	Electronic Micropayment Accounts	43
2.10.7	Electronic Prepaid Cheques or Coupons	43
2.10.8	Electronic Cash and Cheques	44
2.11	Conclusion.....	44

3	Non-Repudiation.....	46
3.1	Introduction	47
3.2	Non-repudiation Background	47
3.3	Goals of Non-repudiation	49
3.4	Non-repudiation Services	49
3.5	Non-repudiation Evidence	51
3.5.1	Types of Evidence	51
3.5.2	Elements of Evidence	52
3.5.3	Validity of Evidence	52
3.6	Roles of Trusted Third Parties	53
3.7	Stages of Non-repudiation	53
3.7.1	Evidence Generation	53
3.7.2	Evidence Transfer	53
3.7.3	Evidence Verification	54
3.7.4	Evidence Storage	54
3.8	Requirements for Non-repudiation	54
3.9	Non-repudiation Protocols	55
3.9.1	Definitions, Assumptions and Notations	55
3.9.1.1	The Communication Channels	55
3.9.1.2	Fairness	55
3.9.1.3	Timeliness	56
3.9.1.4	Involvement of the TTP	56
3.9.2	Non-repudiation Protocols without TTP	56
3.9.2.1	Markowitch and Roggeman Protocol	57
3.9.2.2	Mitsianis Protocol	58
3.9.3	Non-repudiation Protocols with Inline TTP	58
3.9.3.1	Coffey and Saidha Protocol	59
3.9.4	Non-repudiation Protocols with Online TTP	59
3.9.4.1	Rabin's Beacons Protocol	60
3.9.4.2	Zhang and Shi Protocol	61
3.9.4.3	Zhou and Gollmann Protocol	62
3.9.5	Non-repudiation Protocols with Offline TTP	63
3.9.5.1	Zhou and Gollmann Protocol	63
3.9.5.2	Kremer and Markowitch Protocol	65
3.9.6	Non-repudiation Protocols with Transparent TTP	66
3.10	Conclusion	67
4	E-commerce Fraud	68
4.1	Introduction	69
4.2	The Nature of Fraudulent Transactions	70
4.3	The Fraud Process	70
4.4	Fraud Consequences	71

4.5	Fraud Techniques	72
4.6	Fraud Detection and Prevention	75
4.6.1	Data Mining and Neural Networks.....	75
4.6.2	Surrogate Card Numbers	75
4.6.3	Verified By VISA.....	76
4.6.4	Card Verification Value (CVV2)	76
4.6.5	Address Verification Service (AVS).....	77
4.6.6	Merchant Authentication	77
4.7	The Most Commonly Used Anti-Fraud Tools.....	79
4.7.1	CVV2/CVC2	79
4.7.2	Address Verification Service AVS.....	80
4.8	Full Address Verification Service FAVS	82
4.9	Case Examples: The Problems with Existing Solutions.....	84
4.10	Fraud Future	87
4.11	Conclusion.....	88
5	Taxonomy of E-commerce Disputes.....	89
5.1	Introduction	90
5.2	Disputes	92
5.3	Assumptions, Notations, Transaction Elements	94
5.3.1	Assumptions	94
5.3.2	Notations.....	94
5.3.3	Transaction Elements	95
5.4	Dispute Definition	95
5.5	Proof of Completeness	97
5.6	The Taxonomy.....	101
5.7	Conclusion.....	106
6	Online Dispute Resolution	107
6.1	Introduction	108
6.2	Necessity for ODR	110
6.3	Nature of ODR	112
6.4	Development of ODR from ADR.....	114
6.4.1	The Development of ADR.....	114
6.4.2	Subsequent Development of ODR	115
6.5	ODR and E-commerce	117
6.6	ODR Conditions and Mechanisms	117
6.6.1	Building Blocks	118
6.6.2	Schemes.....	119
6.7	ODR Requirements	121
6.7.1	Independence and Impartiality:	121
6.7.2	Publicity and Transparency	122
6.7.3	Language Barriers	123

6.7.4	The Right to a Fair Hearing, and Ability to Respond.....	123
6.8	Dispute Processes	123
6.9	ODR Approaches.....	124
6.9.1	Negotiation	125
6.9.2	Mediation.....	125
6.9.3	Arbitration	127
6.9.4	Evaluation.....	128
6.9.5	Decision Support Systems.....	128
6.9.6	Virtual Courts	128
6.10	Critique Of Current ODR Systems.....	129
6.11	Conclusion.....	133
7	E-commerce Transaction Protocol.....	134
7.1	Introduction	135
7.2	E-commerce Transactions	136
7.3	Protocol Requirements and Components	139
7.3.1	Protocol Requirements	139
7.3.2	Protocol Components	140
7.4	Contract Server	142
7.5	Delivery Server.....	145
7.6	Quality Server.....	148
7.7	E-Commerce Transaction Protocol	151
7.7.1	Notations.....	151
7.7.2	Assumptions	151
7.7.3	Transaction Protocol.....	153
7.8	Soft Product Quality Certification.....	154
7.8.1	The Need for Quality Certification.....	154
7.8.2	The Quality Server	155
7.8.3	The Quality Certification Process	155
7.8.4	Benefits of Quality Certification	156
7.8.5	Commercial Application of Quality Certification.....	156
7.8.6	Quality Certification's Further Research.....	158
7.9	Conclusion.....	158
8	Automated Online Dispute Resolution (AODR).....	160
8.1	Introduction	161
8.2	What is AODR	162
8.3	Motivation for AODR	162
8.3.1	Fairness.....	162
8.3.2	Personal privacy	163
8.4	How AODR works	163
8.4.1	AODR Processes	164
8.4.2	Messages.....	164

8.4.3	Services.....	165
8.4.3.1	The Dispute Resolution Service	165
8.4.3.2	The Advising Service	167
8.5	AODR Plug-in	168
8.6	Reasons for the Success of AODR.....	173
8.6.1	Implementation Independent	173
8.6.2	Protection Against Organized Crimes [Professional Hackers]	174
8.6.3	Time and Resources Optimization:	174
8.7	Enforcing the Result	174
8.8	AODR Providers	175
8.9	Enhancing AODR.....	175
8.9.1	Limitation of AODR.....	175
8.9.2	Reducing the Involvement of TTPs.....	177
8.9.3	Reducing Storage Requirements for the Users.....	177
8.9.4	Support for Users with No Evidence.....	178
8.9.5	Resolution Outcome	179
8.10	Conclusion.....	179

9 E-commerce and E-commerce Fraud in Saudi Arabia: A Case Study 181

9.1	Introduction	182
9.2	The Potential Of The Saudi Arabian Market.....	183
9.3	Current Infrastructure	183
9.3.1	Telecommunication and the Internet:.....	183
9.3.2	Payment Methods:	184
9.3.3	Delivery	185
9.4	Future Infrastructure.....	185
9.4.1	Communication and Internet	185
9.4.2	Payment	186
9.4.3	Delivery	187
9.5	E-commerce and Fraud.....	188
9.6	Verification of the E-commerce Dispute Taxonomy	188
9.7	Validity of the Use of ETP and AODR.....	190
9.8	Conclusion.....	193

10 Conclusion 194

10.1	Introduction	195
10.2	Contributions	197
10.3	Future Research	198

Bibliography..... 199

List of Figures

Figure 2-1: Categories of Electronic Commerce	19
Figure 2-2: Cash Transaction Cycle	27
Figure 2-3: Cheque Transaction Cycle.....	29
Figure 2-4: Credit Card Transaction Cycle	33
Figure 3-1: Ways to Transfer Goods and Money between Customers and Merchants	50
Figure 4-1: Risk Management Pipeline	72
Figure 4-2: Fraud Tools Usage.....	78
Figure 4-3: Current AVS	80
Figure 4-4: Current AVS with Soft Products	83
Figure 4-5: Proposed New AVS (FAVS).....	84
Figure 4-6: Card4Call Statistics for One Year	85
Figure 4-7: 123Callingcards Statistics for One Year	86
Figure 4-8: Level of Concern about Online Payment Fraud	87
Figure 5-1: The Dispute Pyramid	92
Figure 6-1: Dispute Processes	123
Figure 6-2: SquareTrade Mediation Fees(1)	130
Figure 6-3: SquareTrade Mediation Fees (2)	131
Figure 6-4: SquareTrade Mediation Fees (3)	131
Figure 6-5: SmartSettle Dispute Resolution Method	132
Figure 6-6: Cybersettle Dispute Resolution Method.....	133
Figure 7-1: E-commerce Processes	136
Figure 7-2: Contract Server Architecture	142
Figure 7-3: Delivery Server Architecture.....	145
Figure 7-4: Quality Server Architecture.....	148
Figure 7-5: E-commerce Transaction Protocol Architecture	152
Figure 7-6: Time Chart for the ETP	153
Figure 8-1: The AODR System Architecture	164
Figure 8-2: Time Chart for AODR Dispute Resolution Service	167
Figure 9-1: Percentages of Dispute Reasons in Saudi Arabia	191

List of Tables

Table 4-1: Card4Call Statistics for One Year..... 84

Table 4-2: 123CallingCards Statistics for One Year 85

Table 9-1: Saudi Fraud Cases and Reasons..... 189

Table 9-2: Dispute Cases and Reasons in Saudi Arabia..... 191

CHAPTER ONE

Introduction

CHAPTER ONE

Introduction

1.1 Electronic Commerce

The worldwide Electronic Commerce (e-commerce) market is the only one that is still doubling in size year on year and yet at the same time has still not reached its peak. Many business analysts believe that it still has a long way to go before it reaches even this point.

E-commerce was facilitated with the invention of the Internet; technological development has since made it easily accessible and at the same time provides a wide diversity of products and locations, ease in navigation and search, and 24/7 availability.

However, one of the major obstacles facing growth within the industry is that of security, potential customers are not confident about the degree of transaction security when buying or selling online. Even where goods online are cheaper than the same items available in-store or by other physical means, many customers still prefer the second alternative, claiming that their identity and payment details will be more protected outside of the digital world. However this problem is slowly being resolved due to the efforts of researchers and businesses in an attempt to make e-commerce more secure and also to educate users. At the same time many people are now being forced to buy online because of the new products being offered exclusively via the Internet.

1.2 E-commerce Products

The huge potential of the e-commerce market is encouraging many companies to offer new products that are capable of being delivered digitally, for example live music. E-commerce products are mainly divided into two categories: hard, i.e. tangible products, requiring shipment to the buyer. This category covers all traditional products that the consumer will be familiar with such as clothes, toys, computers etc. The second category

is defined as soft, i.e. intangible products those available for consumption without physical shipment. Examples here include software, music and calling time [16].

Soft products may also comprise services such as subscriptions to online newspapers or ISP, the ability to watch a real-time film etc. Some of the more traditional hard products are now converting to soft products due to ease of production and the possibility of making them much more widely available and therefore improving market reach. Such products include books and music CDs.

1.3 E-commerce Fraud and Fraud Prevention

Since the invention of the computer network, ‘crackers’ have been misusing it. For some it is merely a form of entertainment, for others it provides a source of revenue. However this makes any e-commerce site or server vulnerable to more attacks than a normal site where all information is easily accessible to the Internet public.

In order to commit fraud, a person does not need to be a computer ‘expert’. Any Internet user can make a fraudulent purchase, especially in the case of soft products. Those committing fraud do not fear the law since there are no laws governing the entire Internet and it is almost impossible to trace any fraudulent activity back. Low cost and diverse delivery and payment methods of most soft-products make it even harder for merchants to try to get their money or the products back since tracing may cost more than the cost of the product itself [17].

Because of the severe damage some of these fraud cases can cause to the merchants and the payment companies, many fraud detection and prevention systems are now in use. Each of these systems is designed to handle a specific fraud scenario. Currently the most widely used are data mining and neural networks, surrogate card numbers, Verified By VISA, Card Verification Value (CVV2), and Address Verification Service (AVS) [17, 16, 139].

Alternative Dispute Resolution (ADR), which is resolving disputes other than via litigation in the courts, has been used for long time. ADR has proved to be more efficient

than going to court since it is cheaper, faster and is able to provide more satisfactory resolution outcomes. However, most disputes resolved using ADR are concerned with hard-products. Therefore an alternative system for soft-products should be available.

1.4 Fair Exchange and Non-Repudiation

One major feature of e-commerce soft-products and services is the difficulty encountered when trying to revoke or invalidate the transaction. If the buyer receives the product then the merchant has no effective means to force the person to return it. This is particularly true if the merchant and the customer live in different countries with differing laws and regulations.

Usually, the transaction of exchanging the money with the goods must happen at the same time to ensure that both customer and merchant get what they want, but this is almost impossible to do in the electronic world since all transactions need time to travel and will pass through many servers before they reach the final destination. Link speed and congestion are not controlled. Therefore this limitation could allow some fraudulent user to stop or interrupt the transmission before it reaches the other end, giving him an advantage over the other partner.

For this reason many fair exchange protocols have been proposed in the past in an attempt to ensure that neither of the two exchangers will gain any advantage over the other, either the transaction is completed successfully or interrupted.

Non-repudiation services prevent entities from denying that they have sent or received certain information. They must ensure that when PartyX sends some information to PartyY over a network, neither of them can deny having participated in a part or the whole of this communication [89]. Therefore a non-repudiation protocol has to generate non-repudiation evidence [78]. Many applications such as e-commerce, fair exchange, certified electronic mail, etc. are related to non-repudiation.

1.5 Example Scenario

The example illustrated below shows a simple e-commerce transaction that will be continually referred to in the rest of the thesis.

PartyX is the merchant and anything ending with 'X' means it belongs to PartyX;

PartyY is the buyer and any thing ending with 'Y' means it belongs to PartyY.

PartyY needs to buy a piece of software from PartyX. PartyX negotiates the product with PartyY. PartyY agrees and sends to PartyX the payment information. PartyX checks the validity of the payment received using any of the address verification services available. PartyX receives a positive response from the verification service that the address of PartyY is correct and corresponds to the payment method used. PartyX charges PartyY the agreed amount and then sends the software using any soft delivery method such as Email or download. PartyY checks his address and downloads the software from there.

From the above example, many problems clearly exist. The verification method used is not performing the expected verification since it was mainly built to handle hard-products where there is a physical shipping address to verify. However with e-commerce soft-products this verification is not helpful at all. The main problem is that any one who steals PartyY's payment method and knows his physical address can purchase any soft-products he wants and receive it at any designated point.

PartyX has no way to prove the delivery of the goods and has no signed receipt from PartyY to use in any future dispute. Furthermore, if PartyY receives the software and then claims not to have done so or even goes as far as stating that the order was not even placed in the first instance, Party X once again has no evidence of participation or delivery.

1.6 Scope

The ideal situation would be one that enables a buyer to purchase soft-products online and pay for them by any e-payment method. After both parties receive what they want correctly through a soft-delivery method like an email or download, neither the buyer nor the merchant should be able to deny receiving what they expected or participating in the transaction.

In order to achieve this ideal situation, enough evidence should be available to challenge any fraudulent transaction on the Internet using standard Internet applications that all the Internet users know. This thesis will try to solve the fraud in soft-products by a technical solution rather than laws and regulation, since laws and regulation if not enforced by the system, have no authority in the Internet due to its global nature.

1.7 The Proposed Solution

Much of the work that has been done to resolve disputes online is still in progress and many different approaches and solutions have been suggested. However, despite the massive amount of research that has been published and implemented in the past, the aim of resolving disputes efficiently has still not been satisfactorily achieved.

The thesis discusses in detail the fact that previously proposed solutions still suffer from serious flaws that make them unsuitable for certain products or payment methods. The common, and weakest aspect of all the approaches suggested so far is the continued need for human involvement in the dispute process, ultimately leading to higher redress costs.

Apart from the exchange process problems, i.e. those involving money and goods, attention is also paid to other important factors such as timing and quality that are usually neglected in these detection and prevention techniques. Dispute scenarios from many different perspectives will be analysed, viz. computer science, business, legal and that of the participants themselves. From the analyses, all possible dispute cases will be formally listed using the 'Truth Table' approach. This analysis then will led to the design of a comprehensive taxonomy framework for dispute in e-commerce.

The term Online Dispute Resolution (ODR), which is the online technology applied to Alternative Dispute Resolution (ADR), has been used when looking at systems for resolving disputes other than via litigation in the courts, and for those using online technology in particular. Current ODR systems and their suitability for the e-commercial world will be examined and will conclude that not all are appropriate for e-commerce situations (since most still involve a human element and often make the resolution process more costly than the actual item under dispute).

The proposed solution to the problem is by automating the online dispute resolution process. The total solution will be described in two parts (i) an E-commerce Transaction Protocol (ETP) forming the infrastructure where the transaction will take place and be able to accommodate any new improvements in the future, and (ii) an Automated Online Dispute Resolution (AODR) system which should automatically resolve any dispute occurring within the proposed e-commerce model. In order for the AODR to resolve any dispute, a product/payment specific plug-in (add-on) will be incorporated into the system. For illustration purposes, credit cards as a payment method will be selected and the appropriate plug-in specification for soft products and credit cards will be created.

1.8 Structure of the Thesis

The thesis proposes an automated dispute resolution system designed to lower the cost and time of redress. It also explores the possibility of directions for future research and presents these possibilities within the body of the work.

Chapter 2 discusses the nature and development of e-commerce as a form of conducting commercial exchange. The most popular types of e-commerce products are described, together with the most common terminologies for e-commerce transactions. The future potential of e-commerce is then considered. Issues such as trust and security in the transaction process are implicit in the chapter.

The chapter then goes on to describe traditional forms of money as a medium of exchange and how more sophisticated and secure systems of exchange have developed.

Established practices will then form the basis for describing new, emerging electronic methods of payment.

Chapter 3 describes the nature of non-repudiation services and will explore some of the issues regarding evidence such as types, elements and validity and their life cycles. The role of the trusted third party (TTP) will also be considered and will include an examination of the nature and emphasis being placed on their involvement in non-repudiation protocols.

Chapter 4 will provide a critique of current e-commerce fraud prevention and detection techniques. Ultimately it will suggest that not all are suitable for e-commerce and therefore able to provide complete protection against fraud. Emphasis will be placed on analysing the techniques that are used most frequently by identifying their drawbacks and providing suggestions for their improvement. It will conclude by discussing the future of preventing and detecting e-commerce fraud. As a result it proposes certain improvements on current state-of-the-art techniques by focusing on one of the most frequently used fraud prevention methods.

Chapter 5 is intended to present a taxonomy of all possible dispute scenarios in the field of e-commerce. It will analyse scenarios from many different perspectives: computer science, business, legal and also the transaction participants' point of view.

Dispute cases will be studied in general and will not specifically be concerned with any specific goods, payment or exchange methods. All possible dispute cases will be formally listed using the 'Truth Table' approach, and a comprehensive taxonomy framework for dispute in e-commerce will be derived from these possibilities. This taxonomy should provide an adequate basis for ODR system designers and others dealing with dispute resolutions in order to better understand the nature of the online environment.

Chapter 6 will study current Online Dispute Resolution (ODR) systems and their suitability for the e-commercial world in more detail. It will conclude by suggesting that not all methods are suitable for e-commerce transactions with soft products, since in most situations there will be a human element involved in the resolution process, automatically adding more cost.

Chapter 7 will talk about the proposed solution and how in order to solve the current problems in e-commerce dispute resolution a complete solution must be offered. The solution will comprise two parts (i) an E-commerce Transaction Protocol (ETP) that is reasonable and expandable to accommodate any new improvements in the future, and (ii) an Automated Online Dispute Resolution (AODR) system which should automatically resolve any dispute happening within the proposed e-commerce model.

This chapter will discuss the e-commerce transaction protocol in general, its components and how it works. The terminology used is already well-known, the intention is not to create a new technology, rather its intention is to build upon existing knowledge by modifying and suggesting improvements to better satisfy technical needs. It will also demonstrate the new idea of assigning a quality certificate to every soft-product and the beneficial advantages of that.

Chapter 8 will discuss the existence of an effective Automated Online Dispute Resolution (AODR) system, its dependence on an effective ETP, and how the system itself actually functions. For illustration proposes and since the focus of this thesis is about disputes regarding soft products, this chapter selected one of the most common payment methods used in e-commerce, that of using credit cards to create the appropriate plug-in specification for soft products and credit cards.

Chapter 9 will talk about e-commerce in Saudi Arabia and discuss current and future developments. It will then describe a case study that has been conducted in the dispute resolution department on one of the major banks in Saudi Arabia. The case study analyzed more than 500 dispute cases in order to test the viability of both the e-commerce dispute taxonomy and the proposed model. It demonstrated the suitability of using ETP with AODR in order to resolve soft-product disputes automatically.

Chapter 10 concludes by summarizing its original objectives, subsequent research and findings that led to proposals for a new solution, contributions to the current field of academic study and suggestions for future research.

CHAPTER TWO

Electronic Commerce and Payments

CHAPTER TWO

Electronic Commerce and Payments

2.1 Introduction

Over the last five to ten years the growth of Electronic commercial transactions over the Internet, or “e-commerce,” as it has come to be known has been so fast and unexpected that many experts continue to underestimate its growth and expansion. The rate of e-commerce growth continues so rapidly that most of the time projections are outdated as quickly as they are published. E-commerce with all its categories including business-to-customer (B2C) and business-to-business (B2B) transactions is now a significant part of commercial transactions worldwide. Subsequently, policymakers and developers are likely to face more and more complex issues of security, privacy, taxation, fraud, infrastructure development and other issues in the coming years.

This chapter will discuss the nature and development of e-commerce as a form of conducting commercial exchange. The most popular types of e-commerce products are described, together with the most common terminologies for e-commerce transactions. The future potential of e-commerce is then considered. Issues such as trust and security in the transaction process are implicit in the chapter.

The chapter then goes on to describe traditional forms of money as a medium of exchange and how more sophisticated and secure systems of exchange have developed (which in turn have resulted in greater consumer confidence and improved economic growth). Established practices will then form the basis for describing new, emerging electronic methods of payment.

2.2 E-Commerce Definition

E-business and e-commerce are concepts often used in conjunction with the use of Internet technology by businesses and end-consumers. There is a fine but important difference between e-commerce and e-business.

E-business is a means of enabling and supporting businesses to be more efficient and flexible in their internal operations, to work more directly with their suppliers, and to be more reactive to the needs and expectations of their customers. It allows businesses to select the best suppliers regardless of their geographical location and to sell to a global market.

One special case of e-business is e-commerce, in which a merchant provides goods or services to a customer in return for payment. A special case of e-commerce is B2C e-commerce where the customer is an ordinary buyer rather than another business. However, while these special cases are of significant economic importance, they are just particular examples of the more general case of any form of business operation or transaction conducted via electronic media.

Hartman, [14] offers the following definitions which outline the differences:

An e-business initiative is any Internet initiative - tactical or strategic - that transforms business relationships, whether those relationships are business-to-consumer, business-to-business, intra-business, or consumer-to-consumer. An e-commerce initiative is a particular type of e-business initiative that is focused around individual business transactions that use the Internet as medium of exchange, including business-to-business as well as business-to-consumer. Similar definitions exist, e.g. Turban [15]

These definitions differ mainly in scope: e-business is about supporting and enabling business relationships in general, while e-commerce is about business transactions between different companies and/or end-consumers. Another possible definition of electronic commerce would be: any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact.

2.3 History of E-commerce

The history of e-commerce mainly depends on how e-commerce is defined. An argument could possibly be made that the first transaction completed on the telephone or via a fax was the first e-commerce transaction. But according to the definition of e-commerce in the previous section, in 1969 America's Department of Defense commissioned a project called the ARPANET for researching networking and this became the Internet. However, it was used purely as a research tool for more than 20 years. Subsequently, Tim Berners-Lee at CERN developed the World Wide Web which was officially released in 1991 where also the America's National Science Foundation discontinued its restrictions on the commercial use of the Internet. At this time the first Internet business started. The Internet was essentially a world of text only. In 1993, the first graphic web browser, Mosaic, was introduced. The mixture of a World Wide Web, pictures, graphical web browsers, and no commercial restrictions on the Internet, initiated Internet e-commerce.

2.4 E-commerce Products

E-commerce products cover all the current normal products and services and more. A distinction should be made between physical (tangible) goods and electronic goods that can be delivered directly through the Internet (audio, video, images, text, software...).

It is possible to classify e-commerce products into two main categories: Hard-Products and Soft-Products:

Hard-Products: Includes all tangible products that require delivery to a physical address if purchased. Clear examples are laptops, printers, house-wares, clothes...etc. E-commerce represents an evolution of the current method of trading for physical products. It benefits from the new potential offered by technology to improve the efficiency and effectiveness in terms of lower costs, expanding market potential and better meeting customers' needs respectively. E-commerce also improves product and service innovation, especially through the easy interaction between the merchant and customer. Trading for physical goods online is expected to have an enormous impact on competitiveness and quality of services but limited impact on employment.

Soft-Products: This includes all intangible products that can be shipped electronically. The trading of electronic goods (multimedia works, games, etc.) represent a revolutionary new way of trading, since the full e-commercial transaction can be conducted at once online. It could create totally new markets and develop some new industries (such as digital publishing). This highly pioneering form of e-commerce is expected to have an important impact on competitiveness and create “new” employment opportunities.

Before further classifying soft products it is important to define some terms: **Has-cost** and **Has-No-Cost**. Has-Cost means that this product is either expensive or very expensive. For example a pre-paid calling card can be described as being very expensive where as a piece of music can be considered inexpensive (has-No-Cost) because it can be recopied many times over and the cost of copying will be comparably low to its price. Another term to define is traceability. This means a fraud purchase can be **Traceable** if it can be traced for example to a phone number or an official IP address, or **Non-Traceable** if otherwise.

1- Has-Cost-Traceable: The loss in this category is not very high. Often times the cost of tracing is higher than the cost of the product itself as illustrated in the following two examples. Customer service for a laptop company: when the machine is not covered by the warranty, the company usually charges per minute for customer service by asking for a credit card or a bank account. If a fraud happened in this case then the cost was the time of the customer service representative who answered the call, which is quite high some times, depending on the type of customer service he is providing. The cost of tracing this fraud is low since they have information about the original purchaser and, if not, they can add a note in the system to mark this machine as a stolen machine so that the next time someone calls for a service under the same serial number the company will try to get the machine since it is noted as stolen (there are many ways to trace this item, but this is beyond the scope of this thesis). In contrast, if a prepaid calling card is purchased online then the loss is the price of minutes in the prepaid card itself, which costs many merchants 70%-80% of the actual street price of the card. Here the tracing of the fraud is very high since one has to go and see the log for the calls, and if this card has not expired –which is a rare case, since the merchant will not know about the fraud until the real

owner of the card reports it, which is typically one month from the time of purchase - then they find out from where that thief was making his call and subsequently knock on his door and catch him. Let's imagine however that he was using a pay phone or any public phone, in this case there is no way to trace him unless one tries to call the same number he was calling and finds out who called them and where he lives. In many cases this is not possible since most fraud cases involve international calls and also there is no single database to search the called number and identify every person calling it in the immediate area of that pay phone and try to trace them. It is clear in this case that the cost of tracing is high, but an additional condition in tracing is that unless a certain amount of money is stolen the FBI or the authorities will not provide assistance, and that amount is around \$50,000, which means if one has a fraud of less than \$50,000, one has to deal with it through his own lawyer which is quite expensive since the cost of many soft products is on the average of \$20 to \$100 maximum.

2- Has-Cost-Non-Traceable: These are almost the same products mentioned above but the delivery method makes it Non-Traceable. For example, a Calling card pin number is sent to a free email and opened from an Internet café, or from an international location, in such case there is absolutely no way to trace it.

3- Has-No-Cost-Traceable: The loss in this kind of fraud is extremely low and there is no need to waste more money in tracing the thief. One example of this is downloading a piece of music or software. This piece of music or software costs money to generate, but the cost of tracing the fraud is much higher since one has to find the IP address of the thief who downloaded it and trace it. In most cases this thief can be in an Internet Café or in a different country where the cost of one more copy is only the size of the downloaded file divided by the cost of the bandwidth, and this cost almost equals zero.

4- Has-No-Cost-Non-Traceable: The loss in this case is almost the same as in the previous one, but given that it is impossible to trace the thief which is even if it was possible it will not be done. A simple example of this is delivering a picture some one ordered to his email, not by download, in this case with this many free email services and the ease of getting one it is almost non-traceable.

2.5 Categories of E-commerce

In every E-commerce transaction there is a minimum of two parties involved. The maximum number of parties involved could be unlimited but in this thesis the focus is on the two main players in any e-commerce transaction: seller and buyer.

There exists many categories of sellers and buyers but for simplicity will only cover the most important three: consumers, businesses and governments. The seller and the buyer can be from the same or different categories, and this is how the e-commerce categories are defined. In this section each possible permutation of these three categories will be discussed in details.

Consumer to Consumer (C2C): It means consumers selling to other consumers; this form of transaction exists in the real world but it is rare since (i) it will be difficult to find someone who wants what you, the seller, has to offer and (ii) as a result, it is therefore very time consuming. The reality is that usually the only consumers you are likely to encounter in this situation will be friends, family, or flea market traffic. However, this category of e-commerce is now expanding due to the ease of searching on the Internet. These days, you could be in Canada and buy a used laptop or MP3 player from someone in Russia in two minutes. Online auction sites allow the seller to be another consumer. Ebay [58] is one example of the great successful C2C e-commerce sites.

C2C in most cases require a trusted third party to be in the middle of the transaction since it is difficult, technically and economically, for the normal consumer to setup a site to sell or buy items in small quantities. Transferring money from the buyer to the seller is another reason to have the trusted third party involved to complete the transaction.

Consumer to Business (C2B) or Business to Consumer (B2C): The possibility is that in the future this situation could exist: C2B i.e., consumers selling to businesses.

B2C obviously means businesses selling to consumers, usually in the form of online shops or auction sites where the seller is a business rather than another customer. The

B2C category is primarily associated with electronic retailing. This category has expanded greatly with the advent of the World Wide Web. Now shopping malls exist all over the Internet offering all kinds of consumer goods, from food and clothes to computers and motor vehicles.

In the B2C transaction, the seller or merchant usually require the buyer or customer to authenticate his identity and his form of payment. Most of the time the customer's information is not stored with the merchant for security and privacy reasons. Moreover, usually it is a one-time-only transaction, meaning the buyer will never repeat the order, so there is no need to store this information.

Business to Business (B2B): This means just what it says it means: businesses selling to other businesses: factories selling to wholesalers; wholesalers selling to retailers; office suppliers selling to offices; farmers selling to markets, etc. Any transaction between two businesses online is a B2B e-commerce transaction. In B2B companies use the Internet for ordering from its suppliers, receiving invoices and making payments. This category of electronic commerce has been well established for several years using networks and in particular uses Electronic Data Interchange (EDI).

B2B is one of the fastest growing sectors of e-commerce transactions. Business-to-business transactions between small and medium-sized businesses and their suppliers is rapidly growing, as many of these firms begin to use Internet connections for supply chain management, after-sales support, and payments. Most B2B transactions do not require a trusted third party since both businesses have an e-system or at least one of them does. Authentication is also less complicated than with C2C or B2C since most of the time repeat orders are being placed, and trust between businesses plays a vital role in the approval of orders.

Business to Government (B2G) or Government to Business (G2B): The B2G category covers all transactions between companies and governmental organizations. Interestingly, B2G business to governmental marketplaces will presumably be more successful than B2B business-to-business marketplaces. This is because businesses generally prefer to purchase from suppliers with whom they already have a relationship as mentioned above.

Definitely, when businesses need to cut costs, they generally don't look for cheaper suppliers. They demand, request, or work with existing suppliers to cut costs. Governments, in contrast, are usually not supposed to have relationships with suppliers. Such relationships would be alleged at best as bias, and at worst as dishonesty. Governmental purchases need to be based on the merits of the deal - and this is perfectly fitting to on-line marketplaces.

An example of B2G will be publishing the details of approaching governmental procurements over the Internet where businesses can respond electronically. Currently this category is in its infancy, but it could expand quite rapidly as governments use their own operations to promote awareness and growth of electronic commerce.

The G2B (government-to-business) category covers all transactions between governments and businesses. In contrast to B2G, G2B will be less successful since businesses usually hire private companies or individuals to deal with government issues. In addition, G2B is less promising than G2C for the same reason and it is known fact that businesses' needs from government are less complicated and time- consuming than for most citizens who lack sufficient time to leave their work to attend to their needs. Clear examples of G2B will be VAT returns and the payment of corporate taxes.

Government to Government (G2G): The G2G category covers all transactions between governmental organizations. This category is the least important category since governmental organizations usually do not have financial transactions between each other. With the growth of interest in e-government by some countries, G2G e-commerce will certainly be a field that will be given more weight in the future.

Consumer to Government (C2G) or Government to Consumer (G2C): The C2G category is developing. Following the increase of both the business-to-consumer and business-to government categories, governments may extend electronic interaction to such areas as welfare payments and self-assessed tax returns. As a beginning the Governments is already offering the general public the chance to assess their own tax credit worthiness [57].

In commercial terms, G2C means consumers paying something to the government as a return for a service or document. One good example will be applying for a passport or driver license online. Paying one's income tax online is also considered G2C.

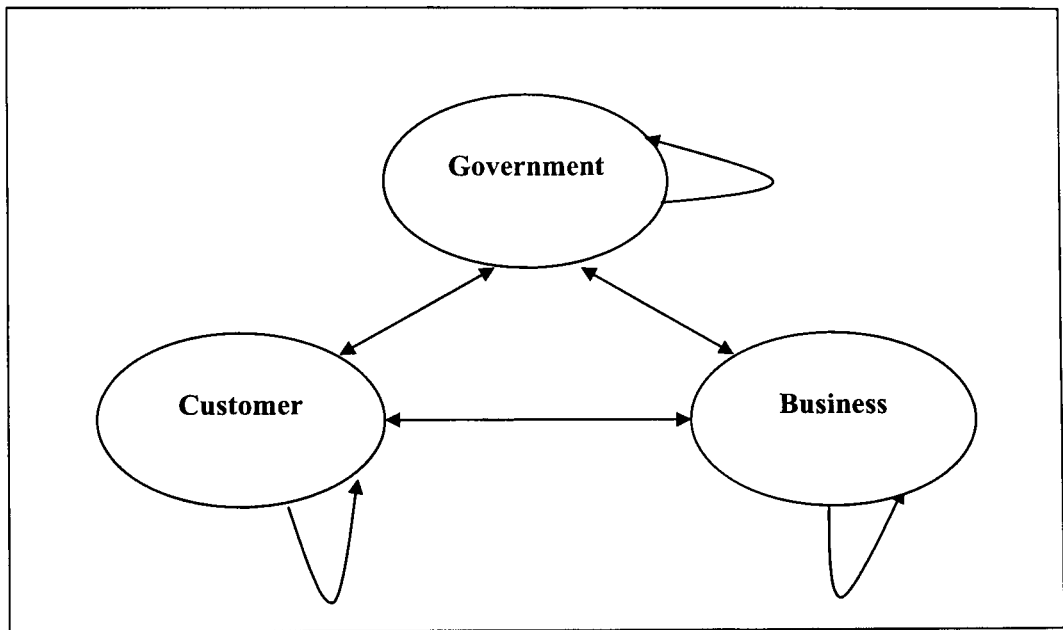


Figure 2-1: Categories of Electronic Commerce

2.6 Future of E-commerce

The way in which e-commerce will develop in the future is uncertain. However two possible major developments seem a possibility.

Wireless Internet, i.e., accessing the Internet and performing transactions over mobile telephones and other highly portable, wireless devices.

Ubiquitous Internet or the disappearance of computers. In other words, an environment where motor vehicles, household appliances, furniture, clothing, office equipment are all connected to the Internet and communicating. A car, for instance, might 'notice' that it is low on oil and book an appointment with the nearest oil changing station and also pay for it.

2.7 E-commerce Security

There are a variety of protection and security concerns that affect e-commerce growth and development. These concerns focus upon detection and prevention of fraud, protection of user privacy and securing transaction information. The most important of these are described below:

Encryption is the encoding of the transaction messages which transfer important information and data. Keys are needed to encode and decode the message. Encryption is an important element of e-commerce security, but the issue of whom and how to hold the keys is still at the heart of the question. In September 1999, the United States allowed the export of unlimited key length encryption products, with some exceptions, in a plan to further relax its encryption export policy. In September 2000 the Bureau of Export Administration in the Department of Commerce issued the rules for implementing this policy. However, the events of September 11, 2001 have caused many in industry and government to review this policy—and the USA PATRIOT ACT of 2001 has given legislators greater authority to gain access to electronic financial transactions data to stop illegal transactions such as illegal money laundering. Concerned about this development, consumers and civil liberties activists will monitor this law closely [92].

Electronic signatures are a means of verifying the identity of a user of a computer system to control access to, or to authorize, a transaction. The key benefit in electronic signatures is enabling electronic signatures to carry legal weight in place of written signatures.

2.8 Trust in E-commerce

Merchants must actively promote trust in e-commerce. The three main ways to achieve this are as follows:

1. Transparency - the merchant should not try to hide anything from the customer. The company name, location, contractual terms, who to contact if there is a problem, use of personal data, etc, should all be made clear on the web site.

2. Providing reassurance and guidance - merchants need to remember that many customers have little experience buying on the web and so may not understand how things work. It is up to the merchant to describe every step of the buying and delivery process. For example, since many customers are hesitant to give credit card information online, the merchant should explain why it is safe to do so and explain alternative methods of payment for consumers who are not convinced.

3. Simplicity - Complicated procedures, unnecessary visual effects, Java-scripting which only work on the latest browsers, web pages which require plug-ins to work (e.g. Shockwave, Real video), all make the buying process more confusing, particularly to the beginner. If someone is confused about what the merchant is doing, he is also likely to be suspicious. Worse, some of these effects can cause the browser to crash. If the consumer is half-way through a transaction and his browser crashes, he is certain to become suspicious of the merchant.

2.9 Payments Methods

2.9.1 Payment Characteristics

For any payment method many characteristics must exist to make it acceptable, some of which are important and without them the payment method will be useless. Some are additional features depending on the kind of payment used and the medium in which it is used.

The following is the list of these characteristics and their meanings, a discussion of each one will be given when the payment method is mentioned. In some situations their characteristics may appear to be in conflict with each other, likewise some are only applicable to certain payment methods. Each one will be defined and for simplicity Sam is considered as a customer, Amy as a merchant or trader, and Tom as an outsider.

Confidentiality/Anonymity/Untraceability/Privacy: Means that Sam can buy something from Amy without Tom knowing. Tom should neither know where Sam buys his goods from nor who Amy's customers are. Even if Tom is a bank, he should not be able to find out that Sam has made two payments or that this transaction was paid by Sam's money [61, 72, 82].

Authenticity: Ensuring that all people and money used are valid. Amy should be able to determine if the money is real money not counterfeit, and Tom as a bank or a mediator should be able to make sure that Sam is the one who made the purchase so he can debit his account and also that Amy is the correct merchant so he can credit her account [61, 63].

Integrity/Security/Reassurance/Confidence: Ensuring that the amount of money in the payment is not altered or modified to benefit anyone, either a party in the transaction or an outsider. For example, Amy and her bank cannot change the amount in the invoice to debit more money from Sam's account [61, 63].

Non-repudiation: Denial of a purchase by the customer in order to get his money back. Sam should not be able to buy something from Amy and after consuming, deny or dispute the charge to get his money back [61, 63].

Confirmation: Both Sam and Amy should confirm the transaction and receive a confirmation notice stating the amount and goods. Sam will know that payment was made and Amy will guarantee payment [122].

Settlement: If Sam's and Amy's banks are not the same, then the process of debiting money from Sam's account and crediting Amy's account with it is called 'settlement' [122].

Divisibility: is the ability to change money into smaller forms of currency. Sam should be able to visit an exchange and change the money he has into smaller units. He should then be able to pay Amy with some fractions of currency if necessary, for example \$2.25 [44, 61, 82].

Offline capability: is the ability to process a transaction without being connected or without contacting the processor for each transaction for authentication. Sam should be able to buy from Amy and pay her without Tom as a banker being involved all the time. Offline also means being able to conduct the transaction without both parties needing to be together in the same place or at the same time [61, 72, 82, 91].

Peer-to-peer/transferability: is the ability to make a transaction between two customers, neither of whom is a merchant. For example, Sam can give his son his weekly allowance without going to the bank or contacting Amy or Tom. Another example is sharing a bill in a restaurant where someone pays the whole bill and the others pay him accordingly; in other words it is where someone transfers money to another without buying anything [91] [61, 82].

Scalability: The money in use should satisfy small value transactions, high value transactions and any future transaction amount [33].

Avoiding Forgery/ Counterfeiting/ Double spending or Re-spending: is the ability to avoid making a copy of money and spend it more than once and in different places [61, 103].

Ensuring Payment/Delivery of goods: is the ability to protect both the customer and the merchant: protecting the customer from paying for something that might not be received, and protecting the merchant from sending goods and not receiving his money [33].

Traceability: is the ability to track the money back to any period of time to help in occasions where it has been used for criminal activity such as drug money or ransom. Traceability can help reveal the identity of the criminals [67, 72, 82].

Detecting Fraud: is the ability to notice and stop fraud before it becomes too serious [67, 72, 82].

User-friendly or simplicity: it should be easy to handle and understand. Both buyer and seller should be able to use it smoothly and easily. One bad example is using heavy money where it is too difficult to carry around [82].

Portability: it should not be linked to a specific location; buyer and seller should be able to move money around and make transactions anywhere [61, 82].

Durability: is the ability to store money for a long time and not lose its value or expire. The value should be maintained until it is lost or destroyed as opposed to merely being devalued. It also should not be easily lost [72, 82].

Acceptability: the form of money should be accepted everywhere or at least in most places to satisfy any size of purchase or transaction [72, 82].

No secret algorithms: the security of the system should not be accomplished by secrecy of the algorithm; the security measures and properties should be freely verifiable [72, 82].

Unit of value freedom: the ability to issue money in any unit and assign a value to it [82].

Online: centralizing the payment process, this requires both Sam and Amy to be connected or be in the same place at the same time. Online sometimes requires Tom to be present as a processor [72].

Transaction cost: is the cost of processing a payment. Most payment systems have no direct costs to Sam, Amy, or Tom acting an intermediary. However, there are many hidden costs. Processing time may also be considered a cost [67, 72].

2.9.2 Contradictions of Characteristics

Some of the above mentioned characteristics are contradictory in the sense that certain conditions can not coexist and if they have to, they will lose some of their significance. These are discussed below, with examples and recommendations for their solution.

Offline and multiple spending: offline spending allows the spender to use his money without contacting a third party. This implies that the person receiving the money has no assurance that it is not a forgery.

Double spending could easily happen in this situation since no one can check the validity of the money until the receiver tries to deposit it or buy something online with it (given that the actual money was already deposited in the bank). If both copies of the money are

handled offline and not deposited then it is impossible to detect the double spending. The worst case could happen when the forged copy of the money is deposited earlier, then it will not be considered as a copy since no one would yet know that there were two copies of the same money in existence. (Money discussed here covers all possible kinds of money which would allow someone to make a copy of the real money and for it not to be detected until both parties are present at the same time or place [61]). A clear example of this is the use of smart cards. If someone was able to counterfeit a smart card then they could buy whatever they wanted until there was a need for an online transaction, or until the real owner detected the unusual charges from his account. In this case both cards would have to be destroyed and a new card would be issued to the real owner.

Transferability and double spending and forgery: This is related to the previous contradiction but is more complex. Since transferability allows anyone to transfer money to another without a third party being involved, the person receiving the money could also be the spender for another transaction without knowing that the money he has received is forged. This is more complicated since it is hard to check when the forgery happened in the transferability chain. With each transfer, the detection of multiple spending or forgery will be delayed. Money laundering and tax evasion also will be hard to detect since the money transactions are not recorded anywhere [61]. Current paper money suffers from this problem since a normal person will most likely not be able to detect forged money: he will spend it and then the receiver will spend it and so on. This could continue until one person decides to deposit it, and then the bank will detect it. In this case it is almost impossible to trace back through the whole chain, especially if the forger was anonymous when he spent the original amount of forged money.

Online and anonymity: since online payment systems require both spender and receiver to be available at the same time or location and since the spender's creditability has to be checked, it is difficult to hide the identity of the spender from either the receiver or the authorities. Therefore, the anonymity of the spender and sometimes the receiver is completely unprotected [61]. Credit card transactions are clear examples.

Online and transferability: online and transferability technically contradict each other since online requires communication with a third party to be involved in the transaction,

and transferability means the ability to transfer money between spender and receiver with no third party involved .[61]. Credit cards suffer from this problem since they cannot be used by someone other than the named credit card holder. So, for example, using a credit card someone can't give money to his wife for shopping or children for their lunch.

Online and Offline: These demonstrate a historical conflict between centralized and decentralized systems. The online system needs to verify all transactions while the offline needs to trust the other party and complete the transaction according to the trust. Offline is a more convenient option for spenders and receivers to use, since it is fast there is no third party involved and it protects anonymity. On the other hand, online systems are more convenient for authorities and financial institutions since they prevent double spending and forgery, and tracing a transaction is easier [72].

Offline and Durability: The conflict here may happen with some types of money. In the offline payment system if the money is lost or destroyed it is very difficult to recover. This is a major durability problem since anyone can use it legally if it is lost and the real owner should consider it as though it never existed [72]. Prepaid credit cards are one example since if lost, anyone who finds them can use them because there is no billing action. Paper money is a much more obvious example.

Anonymity and Traceability: The conflict here is the most complicated and discussed conflict in many Financial and Human Rights Acts. Anonymity protects the privacy of both the spender (not to know where the money is being spent), and the receiver (where the person is receiving the money from). This anonymity is advantageous in certain respects and most people want to have it. However, the negative side of it is the difficulty of traceability. Many people and organizations use this anonymity indecently; fraud is a major problem with anonymity. With no anonymity all customer privacy can be lost since all transactions are recorded. Privacy is not only a luxury, many people ask for it as a novelty but it is often a right and benefit to the individual. Many people have problems because so much information about them is already out in the public domain. The real problem is that these individuals do not know about this risk until they face it and by then it is too late. Another problem with having information about people is the difficulty in controlling who is able to access it. Also, if this is highly controlled then the

individual might not know when his personal data are altered or outdated, causing more problems. On the other hand, due to the high volume of fraudulent transactions and their resultant severe losses it is very important to know who is spending what, where, and when [82]. The most severe thefts and frauds have been conducted using cash since it is highly anonymous and traceability is difficult.

2.9.3 Traditional Payment Methods

In the following section the cycles of the existing payment methods will be illustrated. Their attributes will be compared with the above characteristics and will be discussed in detail.

2.9.3.1 Cash

Cash payment, also known as paper-based payment, has been in existence for centuries and is still used in most transactions today.

Cash transaction cycle

- 1- The customer takes money from his bank or finance house.
- 2- The customer buys goods or services from a merchant and pays the merchant.
- 3- The merchant deposits the money in his bank.

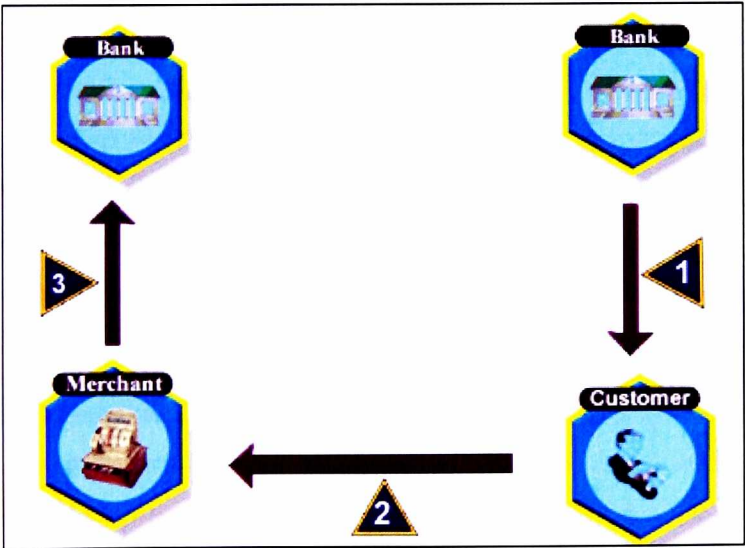


Figure 2-2: Cash Transaction Cycle

Confidentiality and anonymity are preserved in this type of transaction since it is not possible to know the identity of the customer from the cash being used and it is difficult to trace the buyer or the merchant from the cash. Cash transactions have to be in real time and both parties should be at the same place at the same time. This means that the authenticity of the people is definite but the authenticity of the money is not since most people are not able to distinguish between real money and fake money. Integrity, non-repudiation, confirmation, settlement, ensuring payment/delivery of goods, and online are all assured because of the real time behavior of cash (since both parties have to be in the same place at the same time). Cash satisfies the optimum divisibility requirement although some users would still claim that it is not perfect because they would not be able to pay for something that would cost them \$2.559. However \$0.009 is such a small amount that it does not make a big difference in most transactions. Offline capability is very hard since sending the cash by post or leaving it somewhere implies a high risk of losing it; in these situations recovery is almost impossible. Cash is one of the best payment methods for peer-to-peer transferability and also for scalability since it can accommodate transactions of any size. However, it is not fully protected from forgery and counterfeiting even though many new technologies have been deployed to try and counteract this risk. The key issue is that the real security of paper money does not come from anyone knowing the technologies; rather it comes from the difficulty involved in trying to imitate it, which means no secret algorithm. Re-spending is therefore not completely avoided, but the desirable feature here is that the original form of cash will not be lost or damaged because of being counterfeited and it will keep its value. Traceability is almost impossible unless the serial number of each note is recorded during the transaction. Fraud is a serious problem with cash since detecting it requires an expert eye before depositing it into a bank, by which time it would be too late.

Because of its long time in use, wide acceptability and portability, cash is considered the easiest and the most user-friendly method of payment. Durability with cash is confusing, since its ability to last is satisfied to some extent, not like gold but not too bad. However, durability will become very weak since losing cash or damaging it is easy to do, and very easy for anyone to spend when they find it.

Cash can be printed in any currency and nowadays there are more than 100 in existence. Its universal acceptance as a unit of value is guaranteed as long as people agree on its form and value. Cash is still considered the best payment method from a transaction cost perspective and it is usually the cheapest method available to consumers since it involves no third party, processing time, or settlement fees.

2.9.3.2 Cheques

Cheques were probably first used in Italy in the 15th century, but only became the most important medium of exchange in the 19th century. Statistics show that almost 90% of the transactions in the United States used to be conducted by cheques [59].

Cheque transaction cycle

- 1- The customer deposits money in a bank.
- 2- The customer then receives a cheque book.
- 3- The customer buys goods or services from a merchant and then writes a cheque.
- 4- The merchant deposits the cheque in his bank.
- 5- The merchant's bank sends the cheque to the issuing bank (usually clearing houses look at the bank that has issued the cheque book and return the cheque to it) for cashing.
- 6- The issuing bank verifies the signature, debits the customer and transfers the amount of money to the merchant's bank to deposit in the merchant's account.

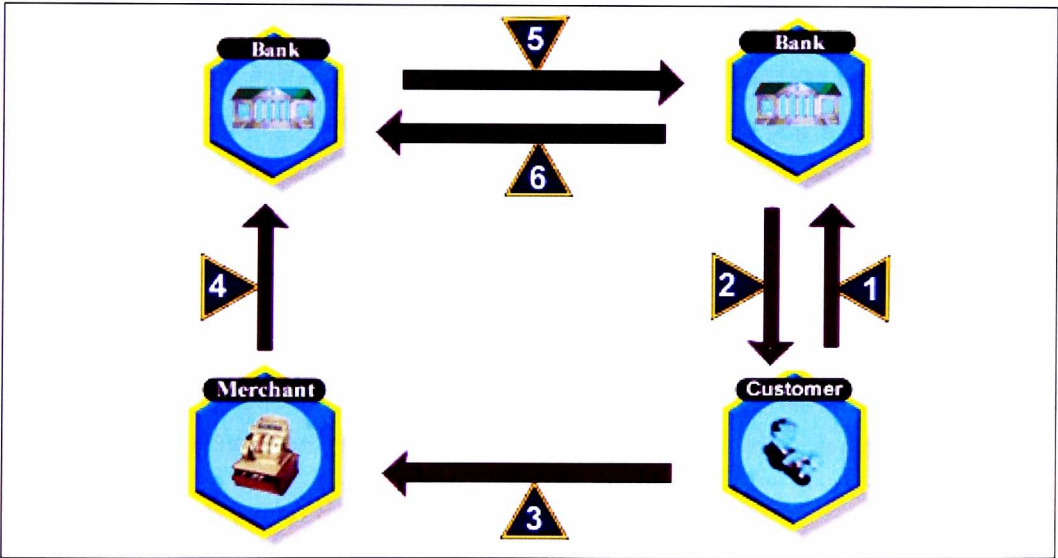


Figure 2-3: Cheque Transaction Cycle

Confidentiality and anonymity is completely lost with cheques since it states the name of the buyer and this person has to insert the merchant's name on it. Therefore, anyone looking at a customer's cheque book will know who was paid. At the same time anyone looking at the merchant's cheques will know the name of the buyer, the amount paid, and sometimes a description of what the amount has been paid for. Authenticity of both buyer and merchant is fully satisfied since the cheque will contain the names of both the buyer and the merchant. However, authenticity of the value of the cheque is not totally secure since the cheque may bounce if there is not enough money in the buyer's account to cover the cheque.

Cheques do not guarantee the integrity of the transaction since the merchant could potentially change the amount in order to get more money from the buyer's account. Without confirmation from the bank in terms of a statement, email or website it becomes more complicated. Some safety measures can be taken when writing cheques, such as writing the amount in numbers and letters, and also leaving no blank spaces before or after the amount. Sometimes including two horizontal lines means that the cheque cannot be cashed directly and should be deposited into the merchant's bank. The length of settlement time may vary if the merchant's bank differs from the customer's bank it can take up to two to three days within the same country, or months if they are in different countries.

Divisibility here is a tricky characteristic since although cheques are considered a good divisible payment method (because you can write numbers and it means money so you can write the smallest amount possible), some people think it is not divisible in the same way as cash since it is not possible to go to an exchanger and give him a cheque for \$100 and ask him to write two cheques to the value of \$25 and \$75.

Cheques satisfy offline requirements since they are much safer to send by post or by courier to merchants than the actual cash. Only the merchant can cash the cheque so it is of no consequence if any outsider knows that the envelope contains a cheque.

A peer-to-peer transaction or transferability is also another tricky characteristic since anyone can pay someone else with a cheque. However, in reality this should not work

since no one else would be able to buy something with the cheque even if it was given to them. Endorsement is what makes using a cheque tricky since you can endorse a cheque to someone else, so for example if Sam wrote a cheque to Amy for \$100 and Amy wanted to pay Tom \$100 she could merely write on the back of the cheque "Pay to Tom" and then sign it. Tom could then deposit the cheque in his account. Many fraudulent transactions happen in this way because in view of the endorsement Tom's bank will contact Sam's to transfer the money from his account to Tom's account. However, no one will check to see if Amy's signature is correct since the only one who knows her real signature is her own bank (which has not been involved in the settlement process).

All sizes of transactions can usually be handled by cheque since there is no limit to the amount a person can write a cheque for except the balance in his bank. Some security measures can be taken in printing the cheques themselves such as printing them on tinted paper, using ink in the printing process, punching a series of numbers out of the paper or embossing them and sometimes using magnetically active ink.

With all of the above counterfeiting possibilities, imitating a cheque is not a difficult job. There are many private printing companies in existence that will print cheques for a small charge if the customer does not want to buy them from a bank. Usually these printing companies ask for an old cheque and a statement (which anyone could easily get from a mail box or rubbish bin). The other step is to be able to copy the signature of the real owner - a much easier possibility than the first example since the person could purchase anything and merely sign the cheque. The buyer can ensure delivery of goods if he asks the merchant to deposit the cheque in his account and not cash it directly, since if he did not receive the goods he can prove that he has paid for it. On the other hand, the merchant can take the risk and send the goods before clearing the cheque to satisfy his customer or he can wait until he clears the check to ensure receiving the payment. Traceability and detecting fraud are usually easy if the owner of the cheque is the one who commits the fraud, but if the cheque is counterfeited or was endorsed many times then valid money which was paid to buy something legal can be 'dirty' by being used to pay for something illegal many times and then cleaned again by buying something legal and finally deposited. Cheques are easy to use because of their simplicity and also they have been

around for many years. Cheques can be carried with people any where regardless of the amount of the cheques or the remaining balance in the bank; so cheques are a portable payment method and the customer does not have to carry cash with him all the time, and meanwhile has full access to the total amount in his account. Cheques are not durable in the sense that the account owner may withdraw the amount and keep his account with no money or close his account, so you can't keep a cheque with you for long time. Losing a cheque is much easier and more durable since it can be canceled easily and get another cheque instead of it. Nowadays many stores accept cheques and some banks even guarantee cheques for some limit written in the back of the debit card of the customer, which guarantees payment to the merchant even if the customer account has no money to cover the whole cheque amount. Some websites and shops accept cheques over the phone or the Internet which makes it not necessary for buyer and merchant to be at the same place and many utility companies use this method for payment and they just ask for a cheque number which you never use. This may show some risk but since most of these companies are well-known companies and usually the money will be deposited in someone's account, it can easily be traced back and recovered from any fraudulent transaction of this kind. Cheques cost a lot more than cash since the transaction time is longer in terms of paying, depositing, and clearing. The cheque book also costs extra money which does not exist with cash transactions.

2.9.3.3 Credit Cards

Credit cards can be issued by many companies; certain retailers issue their own cards to make it easier for customers to purchase and pay on installment. There are two types of credit cards. One type allows customers to pay their bill in monthly installments with minimum interest such as Visa and Master Card. The second type requires the customer to pay the full amount of their purchases at the end of every month, such as American Express.

Diners Club was the first credit card ever to be used. When it was issued in 1950 it allowed its members to be charged for meals at a New York Restaurant. The Bank of America issued the first bank credit card and called it BankAmerica; it is now known as Visa.

In total, the number of credit card holders has increased from around 5 million in 1965 to almost 1.5 billion cards in 2000 and the annual goods charged by credit card reached almost \$1trillion [59].

Credit Card transaction cycle:

- 1- The credit card is issued by an issuing bank to a customer with a fixed spending limit.
- 2- The customer uses the credit card for purchasing a good or service.
- 3- The merchant asks the issuing bank to authorize the transaction online.
- 4- The merchant submits receipts of approved transactions to his bank.
- 5- The merchant bank forwards receipts to the issuing bank.
- 6- The issuing bank transfers money to the merchant’s account.
- 7- The issuing bank periodically sends a bill to the customer.
- 8- The customer pays the bill to the issuing bank.

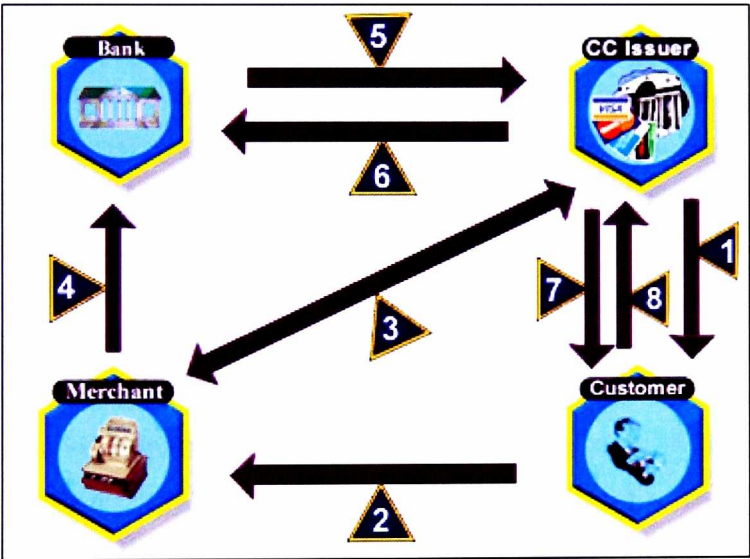


Figure 2-4: Credit Card Transaction Cycle

Confidentiality and anonymity of the customer is completely lost with no privacy whatsoever since each credit card is linked to a person or an organization; even if it is a group card, each card has the name of the holder. This is one of the major problems with

credit cards since by reviewing the buyer's statement all merchants can be identified, and by reviewing the merchant's statement, all customers are also identified.

Credit cards have two main methods of use, either face-to-face as in retail outlets, garages, etc., or remotely as with Mail, Telephone, and Internet Orders (MTIO) which is called Card-Not-Present. Authenticity of both the merchant and customer in the face-to-face system is guaranteed since the customer knows who the merchant is and the merchant can ask for as many 'proof of identities' as needed to make sure that the buyer is the card owner. In remote uses the authenticity is completely lost since there is no way to tell if the caller or Internet user is the real owner of the card or not. Many merchants ask for some information to compare it with the existing information of the buyer in his file with the issuer. Most of the time they will accept the transaction, if it does not seem suspicious, particularly if the goods are to be delivered to a physical address. Integrity of a credit card transaction is guaranteed for both the customer and the merchant if it is face-to-face since both will get a copy of the receipt signed by the customer. In this situation, if there was any error in the amount deposited then both the affected parties can show receipts to solve the problem. However, if the transaction is remote then there is no signed receipt and the customer cannot ensure that he will be charged the correct amount until he receives his monthly statement. Only then can he review it and dispute the charge if it is not correct. Denying a purchase when it has been made will not hold any validity since the credit card issuer is not likely to accept this allegation if the transaction was made face-to-face and has the purchaser's signature. The real problem with repudiation arises when it is a remote purchase, particularly if no goods are to be delivered to the physical address as, for example, in the case of purchasing a piece of soft-product (since the merchant cannot provide proof of delivery).

Settlement of the transaction usually takes place as in Figure 2-4 and it takes around twenty four hours for the merchant to get the money transferred into his account. Issuers bill their customers once every month and the customer has to pay the full amount in the statement within thirty days in most credit cards. Credit cards are not divisible since a customer can not take a credit card with a preset limit of \$1000 and ask the exchanger for two cards to the value of \$500 each. But it can satisfy some of the divisibility

characteristics since it is possible to specify the amount to be paid to the lowest denomination of currency available.

Offline capability is not available with a credit card since a third party must exist to verify the transaction and that the funds required are available on the card. Some companies are prepared to take a risk, ask the customer for information for verification and check it at a later time. Debit cards do almost the same job as credit cards but the difference is that the funds will be taken directly from the customer's checking account. Smart cards are a new extension of the debit card and allow offline transactions by recording some of the important data on a small chip embedded in the card itself.

The merchant swipes the card and asks the customer to key in his password to verify his identity. The merchant can then verify the fund and charge the card; at a later stage the card has to go online to be updated. Peer-to-peer transactions and transfer of funds are not available with credit cards since it is not possible to transfer funds from one person's card to another or pay someone else if they do not have a merchant account. Since most credit cards have a preset limit and the transaction fees are high, it is not really a scaleable payment method. Another problem with scalability is the limited ability to charge huge purchases with it and also it is not worth it to use it for micro payments since the user will be paying fees more than the transaction itself.

Some exceptions for huge purchases exist but these are limited to a special category of person. For example, American Express limits may reach \$3 million if the customer has a favorable credit profile. Credit card fraud is costing merchants, and sometimes customers, hundreds of millions of dollars each year. Fraud can happen for many reasons: first, stolen cards, which represent almost 25% of the total credit card fraud; second, counterfeit cards, where criminals acquire the technology that enables them to "skim" the data contained in the magnetic strip of the card and then manufacture a fake card. This constitutes almost 24% of the total credit card fraud. Third, MTIO, which is the fastest increasing fraud although it only represents 21% of the total fraud so far. Fourth, lost cards constitute 15%. The remaining 15% is distributed to the rest of credit card fraud [16]. As discussed before, the merchant will ensure payment only if he has a signed receipt or delivery notice, otherwise customers can easily dispute the transaction and get

money back from the merchant. In the case of soft products, no proof tends to exist so the merchant can not ensure payment until the dispute period for the customer is reached. Dispute periods usually last 3 months (from the day the credit card holder receives his statement) and sometimes longer. The merchant has to wait from four to eight months to make sure that the transaction is not disputed. On the other hand, the customer is ensured delivery and no liability whatsoever for a purchase that was not made or for goods that were not delivered. Most of the time the customer is liable for transactions even if he did not make them if his card was stolen and he did not stop it by calling the issuer immediately.

Traceability is high since most credit card transactions can be traced back to the correct parties because there is no transferability or anonymity with them. Detecting a fraud and recoverability is easy if it has been committed by a credit card owner (because of the traceability feature). If a fraud comes from an outside user who uses someone else's card some methods can be used to detect it before it happens or stop it from recurring.

For example, if the issuing company has previous knowledge of the credit card owner's behavior in terms of spending patterns, any suspicious transaction can be stopped. If the typical profile involves the owner spending between only \$50-100 a week and then tries to buy an item for \$1000 the transaction can be denied until the issuer confirms validity or otherwise.

Another way to detect fraud is the geographical location of the transaction. It is not possible to buy something from Moscow at 9 am and something else from Los Angeles at 10 pm.

Credit cards are becoming more user-friendly daily because of the ease with which a person can acquire one. Since the credit card itself is not worth more than 20 cents but can allow the customer to use the preset limit on the card, losing a card means losing a plastic card which can be replaced with minimal or no cost. So it is portable but it can not be considered as money.

Nowadays credit cards are widely used and almost all medium-sized shops accept them: more businesses are joining every day. The Internet has opened up a new future for the

credit card since it is now the most popular way of payment and is preferred by both merchant and customer alike. Working online and having the ability to verify and identity are the most popular reasons. On the other hand, one major problem with credit cards are the charges for the merchant, often having to pay between 2-4% of the total transaction amount to the system provider or the gateway, plus certain fixed charges per transaction. These costs limit the use of credit cards for small value transactions.

2.10 E-Payment Methods

The modern developments and technologies have changed the way people pay for their goods and the normal classification of payments, i.e. pay now, later, and before, is not suitable for this era.

Electronic payments can be classified into eight main classes and each class could have a subclass. Some new payment methods may fit into more than one class.

2.10.1 Payment Cards

Payment cards can be divided into credit and debit cards. Credit cards do not draw directly from a bank account, but from a mediator payment account, usually the credit card issuer. On the contrary, debit cards draw directly from a bank account. Debit cards are not widely used on the Internet since the fraud risk is higher than credit cards, but are widely used in Europe for payments made in stores.

Some initiatives are underway to make debit cards available for use on the Internet. Some debit cards are more or less similar to credit cards. Switch [127] is an example of a debit card system that works like a credit card system. Like a credit card, Switch using the magnetic stripe allows for payment with the card present, but also allows transactions using a telephone or the Internet. The only difference in the system with respect to credit cards is that the payment is drawn immediately from a payment account. Because of this similarity, both debit and credit cards can be treated as credit cards when conducting an e-commerce transaction. Someone will notice the difference only when a fraud arises and a dispute is needed.

2.10.2 E-Direct Debit

Direct debit transfers are very popular in Europe: they made up 25.8% in 1999 and 27.3% in 2000 of all non-cash Euro area payments see table 13 of [34]. Typical areas of application include subscriptions and utility bills. In a direct debit transfer, the payer authorises the payee to draw money from his account, usually by putting a signature on an authorisation form. The payee itself initiates the transfer by sending a request to the bank. The bank simply executes the order.

Direct debit authorizations are available in two forms: single and permanent. The single authorizes the payee to draw a specific amount of money from the bank account only once. The permanent is used for recurring charges such as subscriptions, utility and telephone bills.

The vast recognition of the direct debit system has led to this method being applied on the Internet. To do this, a few different methods have been developed:

- Accepting a single mandate for direct debit through the Internet: this method is tricky on the Internet, as no real signature is placed. In order to do it properly, electronic signatures are needed. However, the infrastructure to put electronic signatures is not yet mature.
- Accepting a permanent authorization (with a real signature) offline, and giving the customer a user name/password to pay online: This method is more secure, because a real signature is used but the method isn't entirely Internet-based. The customer buys goods using this user name and password, and then the merchant receives payment for the goods by sending a payment request to the bank.
- Direct debit by a third party: this method is more sophisticated than the first two. The first two methods are not fully electronic, but this one is new in the sense that an additional party (the *intermediary*) is authorized once instead of authorizing each merchant for direct debit separately. Merchants receive payments through this intermediary. This model has two major advantages:

- Only one authorization is necessary for all payments, which makes it less complex to get an offline signature for the authorization.
- The model can easily include payments to private persons (Person-to-Person payment).

2.10.3 Electronic and Mobile Banking.

Bank transfers accounted for 35.7% of all non-cash Euro area payments in 1999 and for 36.2% in 2000³², making it the most popular non-cash payment instrument available. Offline bank transfers are also used frequently on the Internet, but have some drawbacks. One of which is the long time (3 to 7 days) needed for bank transfers to be credited to the beneficiary's account.

The popularity of bank transfers in combination with problems with using offline transfers on the Internet, makes it a logical candidate for creating an online version.

Several methods have been developed, including:

- Electronic and mobile banking
- Electronic Bill Presentment and Payment (EBPP)
- Online bank-transfers

Electronic and mobile banking systems offer the possibility of performing banking actions in an electronic format that traditionally require receiving or sending paper documents, such as submitting a payment order, scheduled payments, buying stocks, etc.

A specific service similar to or part of electronic banking is electronic bill presentment and payment (EBPP). In standard e-banking systems, the payer must enter all the transaction details manually. With EBPP, the transaction details are automatically entered from the electronic bill, and the payer only has to authorize the payment. Some examples include Telecast [132] and Nordea Solo [99].

Very similar to e-banking is the online bank transfer. In an online bank transfer, the account holder, using the Internet, will instruct the bank to transfer money to the merchant's account, which is processed immediately (contrary to the offline bank

transfer). A big advantage of this system is that the payee immediately receives the money in his account. However, this is usually only possible if both the payer and the payee have an account at the same bank. Examples of such systems are Betalen [114] and, again, Nordea Solo.

There are various techniques through which these payment instruments operate; these include:

Voice-telephony: This is the oldest method, but still in use. Account holders make an ordinary telephone call with either the bank's computer, entering data using the telephone keypad, or with an operator.

Direct dial up by modem: As PC's gained popularity, banks wrote e-banking applications that ran on the account holder's computer and contacted the bank by making a modem call. At the time, it was considered more secure and cheaper than having such a system over the Internet, but currently, these systems are losing ground.

Internet: Since the modem system has many disadvantages such as client software, access can only take place from a single PC, consumers connect to the Internet in different methods rather than using traditional modems, etc., banks developed Internet sites for e-banking to replace the client-side e-banking applications.

GSM/SMS: The arrival of GSM phones has made it unavoidable for banks to develop mobile banking systems (M-banking), not only is it now possible to use GSM phones to make voice-telephony calls to banks, but some additional possibilities like performing authentication and using SMS to transfer information between the account holder and the bank now exist.

I-mode and WAP: I-mode and WAP are mobile techniques that provide Internet-like functionality on an advanced cellular phone. Banks are developing e-banking applications for these techniques, but such applications aren't commonplace yet.

2.10.4 Centralized Account Systems

All electronic payment systems involve transferring money to/from accounts. Accounts are traditionally issued by banks and similar financial institutions, such as credit card issuers. However, they may in principle be issued by any other organisation, as an “account” is nothing but a representation of a financial claim that one party has to another.

Transferring money from one account to another is easy if both accounts have been issued by the same party. The reason is that in that case, money transfer is just an administrative procedure, without any “real” money changing place. If the accounts have been issued by two separate issuers, the situation becomes more complex. The same amount must be transferred from one issuer to the other in “real” money. This process is called clearing.

Centralized account systems try to offer a cost-effective and convenient way of paying electronically by avoiding the clearing process. To do this, they make it very easy to open an account and then if someone wants to transfer or receive money he or she is able to. In this way, all transfers remain within the system itself and clearing is avoided. This property makes Person-to-Person (P2P) payment possible in an easy and cost-effective fashion; it also offers security and provides a trust advantage over credit card payments since the customer only needs to trust the centralized account system itself.

However the market for this kind of systems is highly volatile: one of the most famous and successful centralized account systems is Paypal [106]. It currently has approximately 78 million registered users (July 2005), and is available in 56 countries. .

Banks are also entering this market with the additional advantage that the “virtual” accounts can be linked to “real” accounts, facilitating deposits and withdrawals. Examples are Western Union’s www.moneyzap.com and Citibank’s www.c2it.com. Credit card issuers are also entering the market with systems similar to those of centralized account systems, enabling payments between (existing) cardholders. Visa offers its Visa Direct service [138] and MasterCard has formed an alliance with CertaPay to offer P2P services.

2.10.5 Telephony Account Systems

Telephony in general and GSM telephony in particular can be used as a means for electronic payment both for Internet-related and other payments. GSM telephony has a number of interesting properties for electronic payment:

- It can feasibly be used for small payments, whereas other payment types are generally too expensive to use for transfers of less than € 2.
- It is widely available among consumers.
- It's considered to be far more secure than Internet payments.

A telephone can be used for payment in a variety of ways (direct debit, m-banking, centralized accounts). However, in the usage of telephony previously discussed, the telephone was merely a medium. The same holds for integrated solutions in which a (WAP) telephone can be used to make various types of electronic payments. Telephony can be the payment instrument by itself and the telephony account is the related to the payment. There are various models for this and they can be grouped into two major classes: the “premium rate” models and the “direct transfer” models.

Premium-rate models: The merchant has a contract with a telephony operator to provide a phone number where consumer's account will be charged at a much higher rate than when dialing ordinary numbers whenever a consumer accesses the number. Part of this money goes to the mobile operator and the rest to the merchant. The same concept but with some variation is the *premium-rate SMS* where the user has to send an SMS message to a premium-rate number and these numbers cost a fixed amount per message. *Premium-rate dialup* is also another variation with the same concept where consumers need to pay to gain access to a website or a customer service manual. The user charged by the minute for using the site.

Direct-transfer models: A newer model, different from the premium model, works by directly charging the telephony account when a payment has been made. In this case, the telephony account starts to act as a general-purpose payment account. To do this,

payment software installed by the operator may be used to make payments directly from the account rather than through a premium service. For example, a mobile user can buy something and perform payment debited from his pre-paid credit with the operator.

Some examples of telephony payment systems are:

- The Coinlet system by Portalify [108], this system can use both premium-rate SMS, premium-rate voice, or alternatively a 3rd party payment system.
- Mobile2Meter [97], this is a GSM/WAP payment system designed specifically to replace parking meters.

2.10.6 Electronic Micropayment Accounts

Electronic payment accounts are mainly used to solve the problem of paying small amounts of money on the Internet typically from a consumer to a merchant. This distinguishes such systems from those mentioned earlier. This alternative works by aggregating many micropayment transactions together and then paying them all at once rather than paying for each individual transaction.

This method may be used by a single merchant, for example an online audio book store where the audio book value is less than 50P. Hypothetically the merchant could offer this by himself or it could be offered by a micropayment organisation that is trying to work with as many merchants as possible. Examples of such providers of micropayments are Cartio Micropayments [43] and Clickshare [47].

2.10.7 Electronic Prepaid Cheques or Coupons

Electronic prepaid cheques or coupons are similar to the systems above and they may also be used for paying non-micro amounts of money. The most important reason for employing such systems is that they offer the possibility of “prepaid payments” on the Internet. One example of the many businesses that use this method is [www.bon50](http://www.bon50.com). This is a scheme in which a user buys a “cheque” in a retail store. The cheque contains a secret number, much like a prepaid GSM card. By entering the cheque number on the Internet

site of the issuing organization, the user obtains credit that can be spent in a number of Internet stores.

2.10.8 Electronic Cash and Cheques

All the systems described previously work by providing access to some kind of *account*. This may be a credit card, bank account, a telephony account or a micropayment account.

A better technique could be to recreate the notion of *nominal value* on the Internet. In real life, banknotes, coins and cheques written to the bearer can be used for payment by handing them over physically to the payee who will acknowledge their nominal value. An electronic equivalent to this could be called *Electronic Money*.

The forgery problems with such money can be solved over time, the two main e-cash problems are issuing of new but forged money and copying/double spending of existing money. The problem of issuing new forged money may be solved by either using a digital signature or something similar, or by making it computationally extremely expensive to create new money. The problem of copying and double spending may be solved by two ways: (i) maintaining a list of money exchanged for real money or new electronic money and verifying it every time a payment is made, or (ii) by exchanging electronic money for new money after a payment has been received (where the payee can be sure that the money is still good, and that the new money can only be spent by him).

Electronic money has the same great advantage of real money which is protecting the privacy of the users by ensuring that its usage cannot be traced back.

2.11 Conclusion

The intention of the chapter was to discuss the nature and development of e-commerce. It considered the most significant types of e-commerce products and categories and discussed future potential for the emerging technology. Focus was also given to issues such as trust and security in this new technical and commercial paradigm.

In the process it described and identified some of the problems encountered in more traditional methods of payment when conducting financial transactions. It then went on to discuss how the solutions that had been developed to solve these types of problems could be applied to new, emerging electronic forms of payment. These were seen as important in order to avoid mistakes and problems encountered in the past.

Chapter 3 will discuss one of the most significant problems, i.e. that of repudiation, the whole process of denial of involvement in a transaction and the ensuing consequences.

CHAPTER THREE

Non-Repudiation

CHAPTER THREE

Non-Repudiation

3.1 Introduction

In E-commerce non-repudiation services must ensure that when Alice sells something to Bob over a network, neither Alice nor Bob can deny having participated in a part or the whole of this transaction. In order to be able to do this a non-repudiation protocol has to be able to generate non-repudiation evidence.

This chapter will explore some of these issues regarding evidence such as types, elements and validity and their life cycles. The role of the trusted third party (TTP) will also be considered and will include an examination of the nature and emphasis being placed on their involvement in non-repudiation protocols.

3.2 Non-repudiation Background

In case of a dispute (e.g. Alice claiming having sent goods or Bob denying having received it) an arbitrator can evaluate the evidence and take a decision in favor of one of the parties without any ambiguity. With the development of public-key cryptography [140] and digital signatures, the hope of providing non-repudiation evidence was created. Given that an adequate public key infrastructure was possible, undeniable evidence could be based on digital signatures.

The most difficult part in non-repudiation protocols is to prevent one of the two parties involved from cheating and gaining advantage over the other. For example, the merchant getting the money without sending the goods or the customer receiving the goods and not paying for it. A non-repudiation protocol must be fair which means at the end of the protocol, either both entities will have received the expected evidence, or neither of them will have anything that is of value.

In e-commerce, merchants and customers exchange goods and money, this exchange is analogous to computer science message exchange protocol. One of the first solutions providing fairness in exchange protocols was based on a gradual exchange of the expected information [130, 131]. In this series of protocols every party sent a small part of the item he or she wanted to exchange to the other and waited until they received a similar sized part. These parts by themselves would not be useful for either party since they would have to be able to combine all of the parts to read the message.

In order to perform satisfactorily, these protocols need an equivalent or related computing power which in reality is not possible. Moreover, these protocols need a great amount of transmissions.

A better solution is provided via probabilistic protocols [37]. This solution helped solve the problems relating to computing power in the sense that they did not need to be equivalent to or related to their partners, but there was no improvement in the problem of transmission overhead.

A trusted third party (TTP) approach was a new, important and different approach to resolve the problem of fair non-repudiation. The first solution was using inline TTP [48] where the TTP acted as a delivery authority, intervening in each transmission. The intense participation of the TTP created a communication and computation bottleneck. The use of an online TTP was the first improvement to reduce the TTP involvement. The online TTP was involved in each protocol run, but not in each transmission [142, 146]. Offline TTP was a constructive step towards more efficient solutions because in most cases the participating entities were honest and the network functioned well.

In parallel, Micali & Asokan et al. [28, 93] designed an optimistic protocol in the context of certified e-mail and fair exchange. Here the TTP only intervened in case of a cheating entity or a network failure. This approach has also been applied to non-repudiation protocols [83, 143, 144].

The latest improvement in this field has been the notion of a transparent TTP. By only looking at the evidence at the end of the protocol, it is impossible to decide whether the TTP did intervene or not if a transparent TTP is used. However this new development is a

useful feature in e-commerce because it avoids bad publicity since the transparent TTP may intervene due to a network failure, rather than a cheating entity.

3.3 Goals of Non-repudiation

Wrongful repudiations of a particular event or action are of fundamental importance, especially in the commercial arena. Repudiation in communication is defined as “denial by one of the entities involved in a communication of having participated in all or part of the communication” [2]. At the same time, in e-commerce repudiation could be defined as denial by one of the entities involved in an e-commerce transaction of having participated in all or part of the transaction.

In non-repudiation services irrefutable evidence regarding a claimed event or action have to be collected, maintained, made available, and validated in order to resolve disputes about the occurrence or non-occurrence of that event or action [6]. Evidence about the timing of the occurrence of an event or action is required by some non-repudiation services.

In this thesis the events and actions related to an e-commerce transaction in which two parties are usually involved is considered throughout. Those two parties are customers and merchants or buyers and sellers. Most of the time a neutral third party will be involved to make sure the transaction runs smoothly. Since in any e-commerce transaction both parties will send and receive something electronically, i.e. the buyer will send money and receive goods, the merchant will send goods and receives money, a new classification of non-repudiation will be explored.

3.4 Non-repudiation Services

In an e-commerce transaction there are two possible ways of transferring the goods or the money from one party to the other. See Figure 3-1

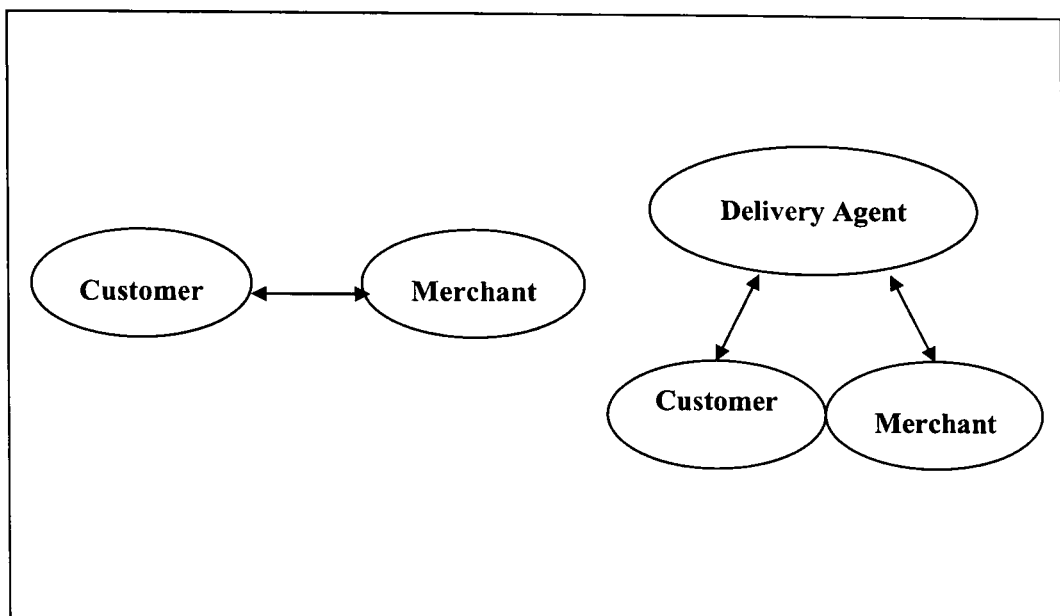


Figure 3-1: Ways to Transfer Goods and Money between Customers and Merchants

The sender A sends to the receiver B directly.

The sender A submits to a delivery agent C which then delivers to the receiver B.

In e-commerce usually the sender and the receiver do not trust each other. This means that in a direct delivery situation the following non-repudiation services will be required as and when there is a need to establish responsibility for actions.

Non-repudiation of Origin (NRO) should prevent the sender, either a merchant or a customer, falsely denying sending the goods or money. NRO evidence are usually generated by the sender or a trusted third party if one is used, and kept by the receiver for future dispute cases.

Non-repudiation of Receipt (NRR) should prevent the receiver, either a merchant or a customer, falsely denying receiving the money or goods. NRR evidence are usually generated by the receiver or a trusted third party, if one is used, and kept by the sender for future dispute cases.

Even in the case of indirect delivery, the delivery agent who is involved in the transfer of money or goods from the sender to the receiver could be a part of a dispute case. Some

evidence is required to support the resolution of possible disputes between the sender and the delivery agent or between the sender and the receiver. In these kinds of instances the following non-repudiation services would be able to provide these:

Non-repudiation of Submission (NRS) should prevent the delivery agent falsely denying receiving submission of money or goods from the sender. NRS evidence are usually generated by the delivery agent and kept by the sender for future dispute cases.

Non-repudiation of Delivery (NRD) should prevent the receiver, either a merchant or a customer, falsely denying receiving a delivery from the delivery agent. NRD evidence are usually generated by the delivery agent and kept by the sender for future dispute cases.

3.5 Non-repudiation Evidence

Evidence is information that either by itself or when combined with other information is used to establish proof about an event or action [8]. Non-repudiation evidence should satisfy the following requirements [145]:

The origin of the evidence is verifiable by a third party;

The integrity of the evidence is verifiable by a third party;

The validity of the evidence is undeniable.

3.5.1 Types of Evidence

Two types of security mechanisms can represent the non-repudiation evidence. First, 'secure envelopes' which are generated by trusted third parties using symmetric cryptographic techniques and formed by symmetric decipherment [90, 120] or by an integrity mechanism [3, 135]. Second, 'digital signature' which is a function applied to the data to be sent to produce a second set of data which will allow the receiver to verify the origin and integrity of the original data [95, 120]. Valid signatures can only be produced by the sender who can be a merchant or a customer, a delivery agent or a trusted third party using asymmetric cryptographic techniques.

3.5.2 Elements of Evidence

Non-repudiation evidence relating to the transfer of goods or money in e-commerce has many elements, some mandatory and some optional which are application dependant. Non-repudiation evidence in any e-commerce transaction usually provides information about the execution of the transaction, the time of the transaction and the parties involved in the transaction, either directly or indirectly. Seven elements of evidence should be specified, (i) the type of non-repudiation service being provided, (ii) the sender and receiver, (iii) who generated the evidence, (iv) any trusted third party involved, (v) the item being purchased or sold, (vi) the timing of the transaction and (vii) the timing of the evidence generation.

3.5.3 Validity of Evidence

The whole non-repudiation idea depends on the evidence gathered. If the evidence does not reflect what has actually happened then the non-repudiation service will not make any progress in resolving the disputes. Most of the pieces of evidence generated are secured from modification or alteration by using private and secret keys. If these keys are broken, revoking them and generating others is a necessity.

Sometimes these keys have a preset validity period after which they will expire. In order for a judge to fairly resolve any dispute, it should be possible to tell whether the evidence was generated when the keys were valid or when they were revoked or expired.

Trusted Time Stamping Parties are used to identify when the evidence was generated, when the keys were revoked, and the expiry date of the key. Usually any evidence generated before the revocation or the expiry of the key is considered valid if it is time stamped by a trusted time stamping party. In [55, 70] many time-stamping services are available.

3.6 Roles of Trusted Third Parties

Trusted third parties play important roles in the provision of non-repudiation services. A trusted third party with respect to security related activities is a security authority or its agent, trusted by other entities [5]. The use of trusted third parties in security services like authentication [4] and key management [7] are widely common. ISO/IEC TR 14516 standardized the use and management of trusted third parties [9, 10]. The extent of the trusted third parties involvement can vary and will be explained more when non-repudiation protocols are discussed.

3.7 Stages of Non-repudiation

Non-repudiation services go through many stages in order to be able to provide the evidence necessary for dispute resolution. As mentioned above the whole non-repudiation idea depends on the evidence, so evidence will go through these stages to be acceptable.

3.7.1 Evidence Generation

Generating the evidence stage is a very important since it is the first stage and without it no other stages will follow. The evidence can be generated by the sender or the receiver using their private keys creating digital signatures. Trusted third parties may also generate and provide supporting evidence if required by the non-repudiation service. In an e-commerce transaction, if a trusted third party works as a delivery agent, then it is required to generate non-repudiation evidence of submission and also non-repudiation evidence of delivery when the goods or money were accepted and delivered. Every non-repudiation service will decide the elements of non-repudiation evidence and the algorithms used for evidence generation.

3.7.2 Evidence Transfer

Transferring the evidence is the most difficult stage in the provision of a non-repudiation service. All the fair exchange problems exist in this stage, so fairness is usually an

important requirement that is hard to get. Without transferring, the evidence has no meaning, since the judge cannot verify it and most likely the fraudulent party will not provide evidence that harm him. So every party in the transaction should have in his possession the evidence he wants at the end of the transaction and no party is in an advantageous position during a transaction. The communication channels reliability can also strongly affect evidence transfer.

3.7.3 Evidence Verification

At any stage during the e-commerce transaction or after it, any party who is interested in the evidence should be able to verify the validity of it as soon as it is generated to gain confidence that the supplied evidence will be acceptable in the case of a dispute. To protect the privacy of the parties involved, only the parties who have the verification key available to them can verify evidence generated through a digital signature. The verifier should check the validity of the evidence by making sure that at the time of evidence generation, the signature key was valid and not revoked or expired. This timing should be generated by a trusted time stamping agent or it will have no meaning in the verification.

3.7.4 Evidence Storage

After the verification of the evidence, the interested party should be able to store this evidence in a secure place. Storing the evidence in a non secure place demolish all the previous stages and may lead to negative results. Most of the times, this evidence will not be used immediately, but it will be kept for future possible disputes. Some evidence will lose its value after some time and it should be trashed. For example, a non repudiation of origin in an e-commerce transaction conducted using a credit card will lose its value after the grace period when the customer can file a dispute.

3.8 Requirements for Non-repudiation

Every entity involved in the non-repudiation service should have a clear picture about the service provided and the way it works. Some requirements have to be fulfilled in order to

provide a complete non-repudiation service. The evidence generator must know the policy used in verification and what evidence are required prior to generating the evidence. Also, the methods for generating and verifying evidence must be available to all the entities that might need it including a reliable clock to obtain accurate time reference. Finally, a time-stamping agent must be available to the evidence generator to obtain a trusted time stamp on the evidence.

3.9 Non-repudiation Protocols

3.9.1 Definitions, Assumptions and Notations

Some preliminary definitions, assumptions and notations regarding the non repudiation protocols will be discussed before studying the protocols in details. It is assumed that Alice and Bob are the two main entities involved in these protocols.

3.9.1.1 The Communication Channels

Three classes of communication channels are commonly used in the literature.

Unreliable channels: no assumptions made about its reliability, so data may be lost, corrupted and never delivered.

Resilient or Asynchronous channels: deliveries are assured according to the data provided, but will be against an unknown time scale.

Operational or Synchronous channels: deliveries are assured for the correct data after a known, constant amount of time, but this type is rather unrealistic in heterogeneous networks.

3.9.1.2 Fairness

Fairness is an important factor in the non-repudiation protocols since it ensures that any one party has any more advantage than any other. There exist many fairness levels, weak, strong, true and probabilistic fairness.

Weak fairness ensures that if Alice does not obtain the evidence she wants, while Bob did, then Alice will receive a proof of this fact.

Strong fairness ensures that at the end of a protocol either Alice got the evidence she wants and Bob got the evidence he wants, or neither of them got any valuable information.

True fairness ensures that the generated evidence are the same whether the TTP did intervene or not, so it is impossible to decide, by only looking at the generated evidence, whether there was a dispute or not.

Probabilistic fairness ensures the fairness with a given probability and it is mostly used when no TTP involved.

3.9.1.3 Timeliness

Timeliness ensures that the protocol will terminate after a finite time, so that no party will wait forever running the protocol fearing losing fairness if it is stopped before the protocol finishes. Timeliness is a practical property that most protocol should have.

3.9.1.4 Involvement of the TTP

TTP can be classified according to their involvement in the protocol.

Inline TTP will be involved in each message's transmission during the protocol.

Online TTP will be involved during each session of the protocol but not during each message's transmission.

Offline TTP should not be involved in the protocol unless there is an incorrect behavior of a dishonest entity or a network failure.

Transparent TTP is an offline TTP that produces evidence in a faulty case indistinguishable from the evidence produced in a faultless case.

3.9.2 Non-repudiation Protocols without TTP

Gradual exchange first appearance was in the middle of the 1980s in order to achieve the exchange of secrets. As mentioned above this approach has two problems, the communicating entities should have the same or an equivalent computing power and the

high transmission overhead. Syverson in 1998 proposed a new protocol [128] for exchanging low value items or information that would lose its value after some time. Information to be exchanged is ciphered and sent with a commitment of the key used to cipher it. Commitments would be breakable after enough amount of time known on the basis of a known computing power. These commitments are called temporally secret bit commitments and could be implemented via a time-lock puzzle [118].

Han [71] proposed a protocol without TTP where Alice sends the item encrypted to Bob and then posts the key in a publicly accessible place like a forum where any information recorded is neither erasable nor modifiable. In the case of a dispute, the judge will check the validity of the information recorded and make a decision. Famous non-repudiation protocols without TTP will be studied next.

3.9.2.1 Markowitch and Roggeman Protocol

This iterative protocol [87] avoids the involvement of the TTP by accepting the weaker, probabilistic version of fairness. In this protocol except at the last iteration, neither Alice nor Bob is more privileged than the other. The protocol works by randomly dividing the item to be sent into small pieces and sending them one by one in a random order. The number which will determine the number of iterations of the protocol is kept secret by Alice and can not be deduced by Bob during the protocol. These pieces do not have any meaning if they are not combined, so the only way Bob can cheat will be by guessing the number of iterations in the protocol which is almost impossible or with very low probability. In this protocol Alice will not find it beneficial to stop the protocol before its end. In the same way, if Bob stops the protocol before the last send he will not gain any profit. The avoidance of the TTP resolves the communications bottleneck problem.

In the case of a dispute, if Alice claims to have sent successfully the item to Bob, she shows to the judge the non-repudiation of receipt evidence for all the iterations. The judge checks Bob's signatures on receipt evidence and also verifies that the whole item was sent by Alice. If all these checks are correct Alice's dispute will be accepted.

If Bob claims to have received the item from Alice, he shows the judge the non-repudiation of origin evidence of all the iterations. The judge checks the evidence of

origin from Alice and verifies that the whole item was received by Bob. If all these checks were correct Bob's dispute will be accepted.

If the probability that Bob decides at the right time, when he receive all the pieces, to stop the protocol equal 'p', the protocol will be p-fair. If an operational channel is used between Alice and Bob, or deadlines are used, Alice and Bob will be able to decide within a finite time if the protocol ended or not and the protocol will finish after an expected number of iterations.

3.9.2.2 Mitsianis Protocol

Mitsianis in [96] proposed a similar protocol to that of Markowitch and Roggeman [87]. The protocol works by Alice sending to Bob the cipher C of the message M under a secretly chosen session key K. If Bob acknowledges the receipt of this ciphered message, Alice adds a padding W to the session key K to compose the key K1. Alice now, as in the previous protocol, splits the key into randomly different size parts and starts the exchange with Bob. For every part Alice sends, Bob has to acknowledge. So Bob does not know when the key will be completely sent. The same observation about previous protocol regarding disputes, fairness and timeliness will be applicable to this protocol. A major difference between the previous protocol and this one is that the value in determining the number of protocol's rounds is static here and dynamic in the previous one.

3.9.3 Non-repudiation Protocols with Inline TTP

Protocols with inline TTP require the TTP to be heavily involved in every transmission. Since all the transmissions go through the TTP, it collects the non-repudiation evidence and then transmits them to Alice and Bob, so in reality it will act as a delivery agent too. These protocols present several disadvantages, requiring the TTP to manage large databases of centralized sensitive information which represent a significant security risk. They also must maintain the messages they forward, as well as the time of each event. The amount of information handled by the TTP is the maximum possible load leading to a bottleneck and a single point of failure. In contrast, protocols with inline TTP can include important information about the sending or/and receiving time of a message into the evidence. This information allows a judge to resolve disputes about late submission.

Certified email protocols [32] were the first places where inline TTP was used. Coffey and Saidha [48] in 1996 proposed a non-repudiation protocol which gave a good understanding and view for using an inline TTP and they also used the TTP as a non-repudiation server.

3.9.3.1 Coffey and Saidha Protocol

In this protocol, the channel between Alice and Bob and the TTP is a resilient communication channel. A time stamp authority participates in the protocol by producing time-stamp for each communication without considering what the content of the received message is. The time stamp authority time-stamps any message signed by the entity with whom it communicates. Partial evidence which is part of the final non-repudiation evidence is used in the protocol.

The protocol starts by Alice getting her non-repudiation of origin evidence time-stamped and also prepares the partial non-repudiation of receipt evidence. Then, she asks the TTP to initiate a non-repudiable communication session. Alice then sends the message with the evidence to the TTP. After that, the TTP send the partial non-repudiation of receipt evidence to Bob, where he should get it time-stamped to form the full non-repudiation of receipt evidence. Bob sends the non-repudiation of receipt evidence to the TTP who will verify it. If all the evidence are genuine the TTP send the non-repudiation of receipt evidence to Alice and the message and non-repudiation of origin evidence to Bob.

The TTP produces and transmits to both Alice and Bob a randomly chosen value associated to each session of the protocol to distinguish different protocol sessions. The protocol ensures confidentiality of the message transmitted by Alice to Bob and also ensures strong fairness, since Alice and Bob never communicate directly but the TTP collects all information necessary and then forwards them.

3.9.4 Non-repudiation Protocols with Online TTP

Protocols with online TTP do not require the TTP to act anymore as a delivery authority, but the TTP will get involved during each session of the protocol. Protocols using an online TTP have been proposed in [54] and [51] but from related frameworks, i.e.

certified emails and electronic payment. Three non-repudiation protocols will be studied here to give an idea of how an online TTP can be utilized.

3.9.4.1 Rabin's Beacons Protocol

In 1983 Rabin [113] proposed the first exchange protocol making use of a TTP and called it the 'Method by Beacons'. The TTP is used in an extremely different way from the norm. In this protocol the TTP called the *beacon* broadcasts at regular and fixed intervals of time a signed message containing a timestamp t , and a random number i in the range $0..n$. Alice communicates directly with Bob and they have to finish a complete round between two beacons broadcasts. The message is signed by the beacon so that its authenticity may be verified. Alice and Bob, then commence the protocol by exchanging signed messages.

Alice starts by sending "If Bob can produce a message (C, t, i) signed by me, and (t, i) signed by the beacon, then I will be committed to *CONTR* as of time t " then Bob will send "If Alice can produce a message (C, t, i) signed by me, and (t, i) signed by the beacon, then I, will be committed to *CONTR* as of time t ". They will continue doing that by adding 1 to the i in every iteration. Intuitively, for any integer i between 1 and N , if the last message in the exchange was from Bob, then Alice and Bob have an equal probability of being committed after the *beacon* randomly choose and broadcast a number.

If the number is less than or equal to i , then both parties are committed. If the number is greater than i , then neither party is committed. If the last message in the exchange was from Alice and the number broadcast by the *beacon* is less than i , then both parties are committed. If it is greater than i , then neither is committed. But, if the number is exactly equal to i , then Alice is committed, but Bob is not. Therefore, the probability that the protocol terminates in a state in which only one party is committed is $1/N$.

Synchronization between Alice and Bob is a very heavy constraint to realize. Therefore the interval between two broadcastings by the beacon must be chosen so that the entity having the lowest computing power can provide the necessary message within the interval. This protocol is probabilistically fair as Alice can decide to stop the protocol

when she receives the signed message from Bob and before sending her signed message. Fairness is only broken if Bob and the *beacon* choose the same value. This situation can happen with a probability equal to $1/n$. This protocol does not respect the timeliness property.

3.9.4.2 Zhang and Shi Protocol

Zhang and Shi [142] in 1996 proposed a protocol using an Online TTP. The protocol idea works by the TTP at a specific time publishing in a publicly accessible place, for example Internet forums, the deciphering keys for the message Alice sent to Bob.

In any dispute case the judge has to contact the TTP and get the information to resolve the dispute. For this reason, the TTP should manage the database of all the keys used and times it was published for all the protocol runs. Information stored in the database should not be deleted too.

The protocol starts by Alice enciphering the message with a session key and with Bob's Public key. Alice sends this message ciphered to Bob and also sends the hash of the same message, but ciphered only with the session key, to the TTP. Since the message arriving to Bob is ciphered using his Public key, he uses his Private Key to decipher it. Bob sends a signed message, which will include the deadline for the TTP, to publish the session key before it or he will not send the non-repudiation of receipt evidence.

Alice checks the deadline time and makes sure she can transmit the session key to the TTP before it expires, otherwise she terminates the protocol, and in this case no one gets any valuable information. If she can transmit the session key to the TTP before the deadline, she signs it and forwards it to the TTP who will be backing-up the message, the signature and the arrival time. The TTP checks Alice's signature and logs the time her message arrived. If Alice's signature is correct and the session key arrives before the deadline, the TTP publishes a message with the session key in to the public space. Then, Bob accesses the public space and gets the session key. If the session key arrives from Alice after the deadline, the TTP publishes a delay message.

This protocol is strongly fair if the communication channel is resilient. Bob can't read the message unless he reads the key from the public place and he can't repudiate his request, also Alice will not get the evidence of receipt from Bob unless she publishes her key. Since there is no set time for Bob to send the request, this protocol does not respect the timeliness property unless a timeout period is introduced to the protocol with a resilient channel.

A strong feature of this protocol is the confidentiality of the message. No one can read the message even after the key has been published since the message has been ciphered by Bob's public key and the TTP will only get the 'hash' of the message and not the actual version.

3.9.4.3 Zhou and Gollmann Protocol

To minimize the involvements of the online TTP in the protocol, Zhou and Gollmann presented a non-repudiation protocol with online TTP [146] that works as follow. Alice sends the message ciphered, protocol session, time-out value, before which she will submit the key to the TTP, and a signed non-repudiation of origin evidence to Bob. Bob checks the incoming message and decides whether or not to accept it. If he accepts it, he sends to Alice the signed non-repudiation of receipt evidence. When Alice receives Bob's message, she sends the key signed to the TTP. This is the only message the TTP receives in the protocol and the only thing to be done is to check the validity of the signature and the time-out. The TTP posts everything to a read-only public directory under its management. Alice and Bob will then fetch the key and the evidence for this key from the directory. This evidence serves Bob as a non-repudiation of origin and to Alice as a non-repudiation of receipt.

It is clear that the involvement of the TTP in the protocol is very minimal and the protocol is strongly fair if the channels are resilient since neither Bob nor Alice will gain any advantage over the other. Alice will not send the Key unless she receives the evidence she wants, by which time Bob will get the evidence he wants too. Bob has to reply to Alice very quickly so she can submit the key before the time-out and also Alice

wants to submit before the time-out, this process confirms that if the channel is resilient the timeliness property will be respected.

This protocol does not ensure confidentiality since the session key and the ciphered message are accessible to any observer. A good improvement to this protocol would be ciphering the first message from Alice to Bob using Bob's public key as Zhang and Shi did in [142].

3.9.5 Non-repudiation Protocols with Offline TTP

The offline TTP will only be involved if a problem occurs, otherwise the two parties can finish the exchange between themselves. Inaccurate behavior by a fraudulent entity or even a network error could be considered as a problem. These types of protocols are also called optimistic protocols since it assumes no problems will occur in most of the protocol runs and rarely when a dispute has happened will the TTP be asked to get involved and complete the protocol with a fair end.

Certified email protocol and fair exchange protocols with offline TTP started much earlier than non-repudiation. Some of these first protocols were presented in [93], [28] and [29].

Since network failures are not under the control of either party it is not fair to blame one party and call him a fraudulent. For this reason a transparent TTP was introduced to supply evidence in the case of a dispute similar to the evidence Alice or Bob would be able to supply. This is very helpful in e-commerce since such disputes may count as bad credit for either the merchant or the customer.

3.9.5.1 Zhou and Gollmann Protocol

Zhou and Gollmann [143] proposed the first fair non-repudiation protocol. The protocol is split into two parts or sub-protocols. First part is the main protocol in which the TTP is not involved. Second part is the recovery protocol, where it will be launched just in case a problem arises. The protocol assumes that the communication channels between Alice and the TTP and between Bob and the TTP are resilient, and there is no assumption about

the communication channels between Alice and Bob (which means it could be unreliable).

Main protocol: The main protocol consists of three messages. First, Alice sends the cipher c and also the decryption key k ciphered with the TTP's public key. Second, Bob sends the non-repudiation of receipt to Alice. Third, Alice sends k to Bob.

If all the messages in the run went smoothly then the protocol would finish after message three and both parties would be happy. If Bob did not send the non-repudiation of receipt in the second message then nothing would happen since he would still not get the key k . Only if Alice did not send the third message would a problem happen since she has the non-repudiation of receipt and Bob still does not have the key k , in which case Bob would launch the recovery protocol.

Recovery protocol: the recovery protocol activated by Bob sending a recovery request to the TTP. The TTP decipher by its private key the decryption key K received from Alice and sent back to Bob with its non-repudiation of origin. Bob now has the key and Alice has the non-repudiation of receipt. Bob can launch the recovery protocol just after the first message in the main protocol and never send the second message with the non-repudiation of receipt, in this case Bob will get the Key K and Alice will not get the non-repudiation of receipt. For this reason, Bob has to send the non-repudiation of receipt with the recovery request so the TTP will forward it to Alice during the recovery.

According to the definition of fairness, the protocol is fair since both Alice and Bob will get what they want or get nothing valuable. A tricky problem could occur if Bob never sent message two intentionally or because of a network failure to Alice. In this case Alice will be in a position where she can't stop the protocol, since Bob can launch the recovery and get the Key K , and she can't activate the recovery protocol since she is not allowed to do that in this protocol. This is a serious problem for Alice and it could be unfair for her since Bob has now an advantage over her.

3.9.5.2 Kremer and Markowitch Protocol

Zhou proposed using a big enough timeout period to resolve the above problem in his protocol, but what is the limit for “Big Enough”. Kremer and Markowitch [83] proposed a fair non-repudiation protocol, which respects both fairness and timeliness with channel qualities similar to the previous protocol. The idea of the protocol is to have an abort protocol in addition to the main and the recovery protocol.

Main protocol: The main protocol has four messages. In the first message, Alice sends the cipher c , and the evidence of origin for the cipher. In the second message, Bob sends the evidence of receipt for this cipher. The third message is sent by Alice and it consists of the key k and the corresponding evidence of origin. The fourth message comes from Bob and it has the evidence of receipt for the key k .

If Bob does not send the second message before a fixed timeout time, Alice will launch the abort protocol.

Abort protocol: The abort protocol will be launched at any time by Alice. The TTP makes sure that the protocol has not been aborted or recovered before. If never aborted or recovered, the TTP will inform both Alice and Bob that the protocol has been aborted and abort the protocol. Since also a successful protocol never been aborted and recovered, Alice could launch the aborted protocol even after the protocol completed. This does not affect any party since the abort evidence does not mean that the exchange did not take place, but it means that recovery will not be accepted any more by the TTP.

If either the third or fourth messages do not arrive, the affected party can launch the recovery protocol.

Recovery protocol: The recovery protocol here is similar to the recovery protocol by Zhou above but here it can be launched by either Alice or Bob while in Zhou’s protocol only Bob can. After the first message of the main protocol, Bob can launch the recovery protocol since the TTP at this stage has the key K and the non-repudiation of origin evidence from Alice. On the other hand, Alice can only launch the protocol after the second message of the main protocol arrived. Before that, the TTP has no non-

repudiation of receipt from Bob. The recovery protocol will provide evidence of non-repudiation of receipt, origin for the cipher and the key k to Alice and Bob respectively.

Only one of the two protocols recovery or abort is allowed in a single run, this is called mutual exclusivity and it is managed and guaranteed by the TTP since it is involved in each of them. The fact that at any moment Alice and Bob can launch the abort protocol and terminate the protocol run makes this protocol fair and respect timeliness.

3.9.6 Non-repudiation Protocols with Transparent TTP

Offline TTP gets involved in case a problem occurs during the communication between Alice and Bob, this problem can be due to a fraudulent action from either Alice or Bob or a network failure. In previous protocols the TTP digitally signs all the evidence sent by it to Alice or Bob. In case of a dispute these evidence will be used in the resolution. Some applications may suffer from this since a judge will have a negative view about one party in the dispute thinking that he/she is a cheater. For example, in e-commerce if a customer does not pay or the merchant does not deliver the goods this is counted as a negative point. This may affect his future reputation and his ability to do more e-commerce transactions. For this reason, transparent TTP are used to generate evidence in case of a problem completely similar to the evidence generated by both parties in case of a normal run, so by only looking at the produced evidence, it is impossible to decide whether the TTP was involved or not. If a dispute happens the judge cannot distinguish if the evidence came from the TTP or the party itself. This way will make it hard for the judge or any one to blame Alice or Bob for cheating since they have no proof of that.

The use of Transparent TTP was first proposed by Micali [93] in the framework of certified e-mails. Asokan et al. [27] and Bao et al. [36] proposed protocols in the framework of fair exchange. Most proposed protocols were inefficient. Boyd and Foo [40] broke one of Asokan et al protocols and proposed a fair exchange protocol for electronic payment but it was also inefficient. Markowitch and Saaednia [88] came up with the most efficient protocol for fair exchange with transparent TTP which was based on a specific signature scheme (inspired by the Girault-Poupard-Stern signature scheme [111]).

Markowitch- Saaednia protocol [88] consist of four sub protocols, main, abort, recovery, and error. All except error are similar to the sub protocols mentioned above. In the recovery protocol the TTP send evidence similar to the evidence that were supposed to be sent by the other party if it was a non anticipated failure. In the case of an anticipated failure, the recover protocol moves to the error protocol which informs the fraudulent party that this attempt to cheat has been detected and also warns the other party. This protocol is almost similar to the above offline TTP protocols, so it is fair and in this respect, timeliness. The characteristic of not being able to tell that the evidence are actually coming from the TTP or from one of the parties makes the protocol not only fair but provide strong and true fair.

3.10 Conclusion

This chapter has examined the issue of non-repudiation as a means of providing adequate evidence in the case of arising disputes. In non-repudiation, evidence is the most critical since it is the outcome. Therefore, aspects of this evidence such as elements, types and life-cycle have been explored. Some of the most well known protocols have been discussed and their ability to provide non-reputability, ensure fairness and respecting timeliness examined.

E-commerce brings many challenges to these non-repudiation protocols. As a result new fraud cases and dispute types may arise. The next chapter will talk about these e-commerce frauds and the current strategies used to resolve disputes.

CHAPTER FOUR

E-commerce Fraud

CHAPTER FOUR

E-commerce Fraud

4.1 Introduction

As discussed in an earlier chapter, the main focus of the thesis is on soft products fraud. With the growing demand for soft-products that can be delivered via the Internet, e.g. downloadable movies, music, software, and prepaid phone cards, the prevention of fraudulent transactions is becoming increasingly important.

There are many reasons for the rise in the number of fraudulent transactions, the most obvious being that merchants cannot see the customer to verify an ID or signature. This problem existed before the Internet in both mail order and telephone order systems (MOTOs), where both were subject to the same types of problems that Internet orders have today. In addition, however, E-commerce also allows customers to conduct transactions without physical interaction, and the Internet facilitates soft-products and services to be acquired via soft delivery methods: email, download or logging in.

Before eventually going on to discuss a proposed solution it is necessary to explain the major assumption that underlies the text of the chapter. Since credit card use is the major payment method on the Internet, accounting for 88% of all transactions, and since most of the alternatives are still in the early stages of development, the rest of this thesis assumes this is the main method being used when issues concerning payment are being discussed [23].

This chapter will provide a critique of current e-commerce fraud prevention and detection techniques. Ultimately it will suggest that not all are suitable for e-commerce and therefore able to provide complete protection against fraud. Emphasis will be placed on analysing the techniques that are used most frequently by identifying their drawbacks and providing suggestions for their improvement.

It will conclude by discussing the future of e-commerce fraud prevention and detection, and propose certain improvements on current state-of-the-art techniques by focusing on one of the most frequently used fraud prevention methods.

4.2 The Nature of Fraudulent Transactions

Fraud is costing merchants and sometimes customers hundreds of millions each year. Credit card fraud can happen in many ways: stolen cards dominate and currently represent almost 25% of the total credit card fraud. The second most popular method is via the use of counterfeit cards: cards that, once the criminal has acquired the technology, allow him to “skim” the data contained in the magnetic strip of the card and then manufacture a fake card. This constitutes almost 24% of the total credit card fraud. A third method is through the Mail Telephone and Internet Order (MTIO) system, this is the fastest growing method, and currently represents 21% of total fraud. A fourth is via lost cards, constituting 15%; and the fifth, accounting for the remaining 15%, is through minor credit card issues [137].

4.3 The Fraud Process

The outcome of many credit card frauds is linked to the concept of ‘charge back’ i.e., a “returned transaction resulting from the lack of adherence to the conditions of the sales agreement, association regulations, or these operation procedures, that results in the debiting of the merchant account [121]”

Charge back is usually a result of the cardholder disputing the charges in his statement, and according to some statistics 90% of the disputes end in favour of the customers over the merchants. This is because on many occasions the transaction might have had suspicious elements, such as shipping to an address that differs from the billing address, (which accounts for almost 45% of MTIO credit card fraud cases) and when the dispute is finally honored, the merchant has to be responsible for the charges. Whilst some

investigation by the credit issuer then has to take place to find out who received the merchandise, in many cases, specifically those concerning soft products, this type of investigation will not result in a successful outcome since the products would not have been physically shipped.

4.4 Fraud Consequences

E-commerce fraud techniques affect the e-commerce community in many ways, some are directly related to the incident itself, some are indirect. The direct consequences of a fraud include loss of the value of the actual item being purchased, e.g., a calling card access number for £20. It could also include the charge back penalty, which most merchants would have to pay when a dispute arose against them.

The cost of returning the money to the customer is another direct consequence, usually costing the merchant more than the original value because the issuing bank inevitably claims a higher rate for crediting a card than debiting it.

The number and types of indirect consequences are very difficult to estimate. However some of the main factors are mentioned here. As a result of fraud, merchants have to continually review orders. In spite of all efforts to successfully automate this procedure, shortcomings still exist and as a consequence merchants still have to review them manually. This in turn incurs additional employment costs, delays the whole process of approval and ultimately results in reduced levels of customer satisfaction and profit. At the same time the merchant will be required to pay for prevention and detection tools in order to prevent further fraud, resulting in even higher costs.

Another major indirect effect is the concept of 'Valid Order Rejection', resulting in the possible rejection of a transaction placed in good faith on the grounds of suspicion of fraud. According to the 2005 Annual Fraud Report by Mindwave Research [115], 6% of all orders were rejected by merchants, however some of these were valid transactions. The bad publicity and reputation generated from fraudulent cases also affects merchants indirectly.

To stress the seriousness of the problem, Figure 4-1 taken from the Mindwave Research Report presents a ‘risk management pipeline’ where, in practice, the process could be even longer and have even greater ramifications than those described above.

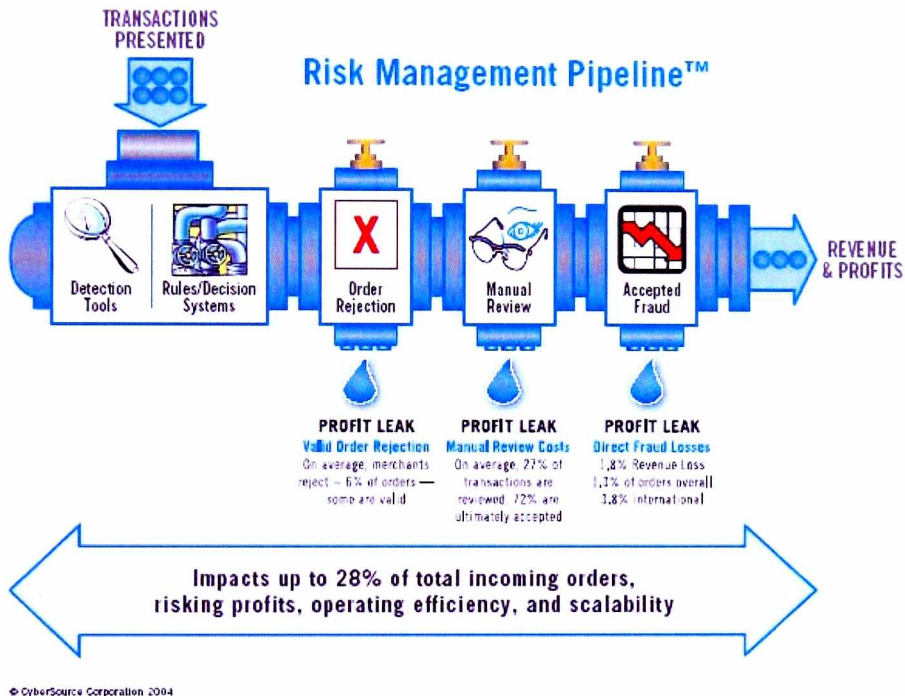


Figure 4-1: Risk Management Pipeline

Source: [115]

4.5 Fraud Techniques

E-commerce products were defined in chapter 2 as either Hard: those requiring delivery to a physical address e.g. printers; or Soft: all intangible products that could be shipped electronically.

Has-cost-soft-products were high cost, e.g. pre-paid calling cards, whilst a piece of music was a *Has-No-Cost-soft-product*, since it could be recopied many times and the cost of copying would be comparatively very low to its price. *Traceability* was the term used to describe a situation where a fraud purchase could be traced e.g. to a phone number or an official IP address, whereas *Non-Traceability* implied the opposite.

Although there are many kinds of credit card fraud, the emphasis of this thesis is on the type of fraud that can occur with the first type of Soft-product, i.e. those defined as Has-Cost and at the same time are Traceable.

The information needed to charge a credit card is only its number and the expiry date. However merchants usually request more information to avoid fraud. For example, the information required for some online systems to approve an order can be as follows: first and last name, address, phone number, email address, credit card number, expiry date and the customer service number of the credit card issuer.

Fraud cases can happen, for example, if someone already has your name, credit card number, expiry date and billing address. In this situation the current online merchant system will check two things: (1) if the credit card number is a valid number, and (2) if both the first 5 digits of the street address and zip code match those in the issuer's database.

This information is very easy to obtain, even from a home mailbox or any online transaction that has been conducted before. Even if the fraudulent party does not have the customer's name, the order can still be accepted if the address and zip code match up. In this kind of situation the transaction might seem to be a non-fraudulent order, but to be able to confirm this, the merchant then needs to call the phone number on the order.

In this situation the fraudulent party might have done one of 3 things:

- Used the real phone number connected with the card, in this case the merchant would know it was a fraud if he then phoned it. However on trying to make contact there might have been no answer or merely an answering machine, in

which case the merchant would have to make a risky decision about whether to approve the transaction or not;

- Used a fake number where the merchant will get no answer when calling, it is then up to the merchant to cancel all the pending-approval transactions up to that time;
- Used someone else's or a public telephone number giving instructions to call at a certain time (since he will not be available at the home contact number). The merchant then has to call in order to verify the information and approve the order.

To avoid any of these possible outcomes, the merchant will quite often ask the customer at the time of ordering to quote the phone number he listed with the credit card company when originally applying for the card. However, there is a tendency for many customers to forget the number they originally used, in which case the merchant must ascertain this information for himself. If the subsequent investigation discovers that the quoted number does not match the customers, he must re-request the correct number from the customer. The major problem with all of this is that banks are not inclined to give clues to merchants as to customer phone numbers – not even the last 4 digits.

A further problem might be that whilst the merchant does have the correct number the person answering the call to confirm the purchase order might turn out to be a different member of the family e.g. teenage son, or even just someone visiting the family home.

'Friendly Fraud'[38] is a very simple concept. this happens when the real owner of the card disputes the charge and claims that he did not order whereas in fact he has. In a situation like this there is absolutely no way for the merchant to convince the credit card issuer that the customer is not telling the truth. At this point the credit card issuer will ask for signature on the receipt (which the merchant has not actually received or asked for since it is soft delivery).

4.6 Fraud Detection and Prevention

The problem of credit card fraud is an issue of great concern for business, the IT industry as a whole, academia and regulatory authorities. Because of the severe damage some of these fraud cases can cause to the merchants and the payment companies, many detection and prevention systems are now in use. Each system was made to handle a specific fraud scenario and target certain aspects of this multi-faceted problem.

This section provides an outline of each of these systems, whilst section 4.7 focuses more specifically on those most commonly used at the moment.

4.6.1 Data Mining and Neural Networks

Data mining approaches [104] and neural networks [68, 112] are designed to gather information pertaining to all of the credit card transactions of a particular customer in order to build up a history of purchasing habits. This information then enables credit card issuers to block any transaction that looks suspicious, whether in terms of the amount being spent or the geographic address. However, this approach does not help Internet based activity since it is diverse in location and at the same time, the value of most soft-product transactions will not be high enough to trigger searches using such systems.

4.6.2 Surrogate Card Numbers

Microsoft, Orbiscom Inc, and Cyota [41] came up with a technology to prevent online credit card fraud by replacing user real card numbers with ‘surrogates’. The replacement number can be used only for a given number of online transactions, after which it becomes invalid. Microsoft surrogate card numbers are very complicated to use if the allowed number of transactions are small and are likely to suffer the same types of fraud problems described so far if the number is set to a higher limit.

A major shortcoming with both the Microsoft Surrogate Card and Verified By VISA systems (see below), is that at the checking out stage a window automatically pops up asking for confirmation of user name and password. This can easily be emulated by a

fraudulent website which will be able to get all of the credit card information, the username and password.

4.6.3 Verified By VISA

VISA claims that the ‘Verified by Visa’ system enhances existing card use with a personal password. When shopping at participating online stores, the customer enters a password in the same way a PIN would be entered at an ATM. The implication here is that only this person can use the particular Visa Card online, thereby providing the same assurances as when using the card in a physical store [139].

As a result, fraudsters are prevented from committing fraud at the checkout stage and purchasers are prevented from committing “friendly fraud” by later denying their transactions. In this case the responsibility will usually be transferred from the merchant to the customer, since he/she should be the only person knows this password. However, there is one important factor that has been overlooked: it is much easier to create a fake website than a fake ATM.

4.6.4 Card Verification Value (CVV2)

Card Verification Value (CVV2) [31] is a unique three or four digit number on the credit card; most credit cards are now required to have this number. It can be verified on real time by almost all MTIO merchants and is supposed to help merchants verify that the customer who is making this purchase actually has the card physically with him.

CVV2 can lose its purpose if it is used everywhere, since in almost all the cases where fraud can happen, the fraudulent customer can acquire and continue to use the necessary information [16]. CVV2 is like any other piece of information that consumers provide on the web: after some time it will be public in the same way as a credit card number and if someone steals the credit card then the number is conveniently on the card.

4.6.5 Address Verification Service (AVS)

Address Verification Service (AVS) is a real-time checking device where the cardholder confirms the first 5 digits of the street address number and zip code to verify that the billing address of the customer matches what is stored with the credit card issuer.

This ensures that the merchants will not risk the possibility of the customer ending up disputing the transaction. It is the responsibility of the customer to ensure that the merchandise is delivered to his billing address, even if he did not sign for it.

Whilst this is supposed to be the best method to fight credit card fraud, in the case of soft-products it is clear that this is not really helpful since no shipping occurs at any time [17].

4.6.6 Merchant Authentication

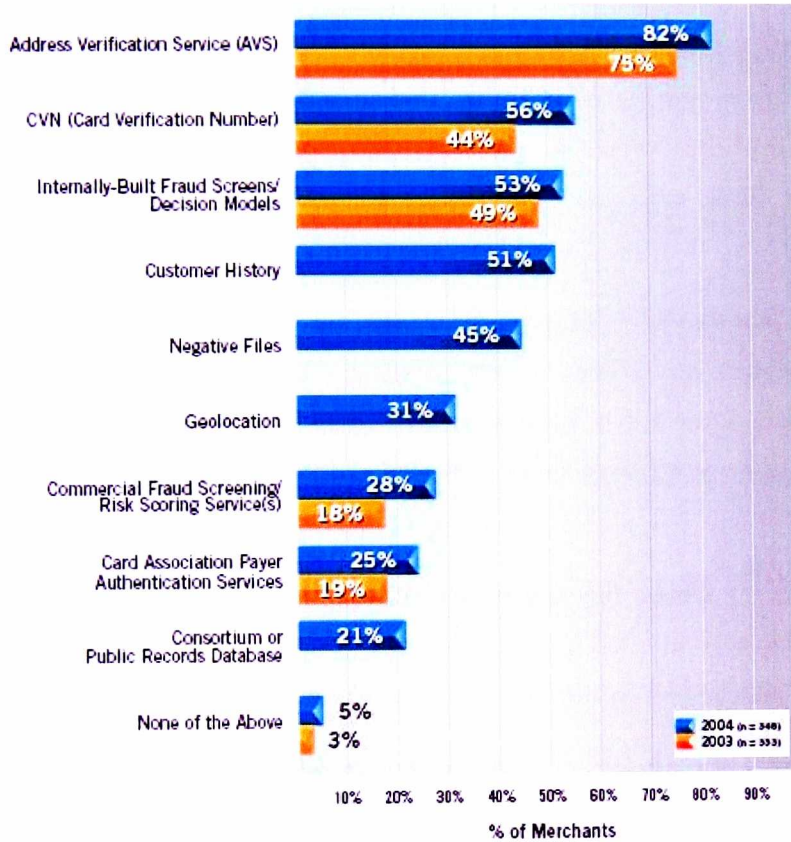
Fraud can also occur as a result of hackers using the merchant payment system to charge customers or credit some accounts. Various techniques are used to prevent such frauds:

Valid Referrer URLs, allowing the merchant to specify the URL(s) from which his payment processor allows a transaction to take place. The processor will reject attempts to process transactions from any other URL. Most of the time merchants are allowed to set more than one URL [62].

MD5 Hash is additional verification tool where a unique signature or fingerprint is created to authenticate every transaction that is processed [117].

Figure 4-2 below shows the extent and nature of increase in use of fraud tools between the years 2003 and 2004.

Comparison of Tools Used 2004 vs. 2003



Fraud tool usage is increasing

Figure 4-2: Fraud Tools Usage

Source: [115]

4.7 The Most Commonly Used Anti-Fraud Tools

4.7.1 CVV2/CVC2

Card Validation Code (known as CVV2 for Visa, CVC2 for MasterCard, and CID for American Express) is a unique three or four digit security number on the credit card. It appears in reverse italic at the top of the signature panel on the back of the card, or just above the end of the credit card number on the front of the card. Most credit cards are now required to have this number.

This number can be verified in a real time by almost all MTIO merchants and is designed to help merchants verify that the customer who is making this purchase does have physical possession of the card. As a deterrent, fraudsters must be capable of providing both the credit card number as well as the card validation value in order to successfully complete a transaction.

All MasterCard cards, both credit and debit, were required to contain CVC2 by January 1, 1997 and all Visa cards were required to contain CVV2 by January 1, 2001. For simplicity, all will be referred to as CVV2 in the remainder of this section.

The CVV2 is designed to have different responses: transactions with a valid CVV2 code will return a Match response; transactions with invalid CVV2 codes will return a No Match response. If a transaction is flagged as a recurring billing, credit, authorization only or capture of a previous authorization, the CVV2 field will be ignored and the CVV2 response code returned will Not Be Processed.

However the CVV2 can lose its purpose if it is used everywhere, since in almost all the cases where a fraud can happen, the fraudulent customer can have it. For example, if the thief stole the card physically then he has the CVV2, also if he hacked into an online system or sniffed a connection then he will also obtain the number. So this number will only help for a certain period of time and it will then lose its value. Therefore use of the CVV2 does not help with soft-products fraud very much.

4.7.2 Address Verification Service AVS

In this service (see Figure 4-3), a real-time checking of the cardholder’s first 5 digits of the street address number and zip code is performed. This will verify that the billing address of the customer matches that stored with the credit card issuer by returning a response code. The AVS response code is sent to the merchant (match or no match), after screening, the Merchant chooses to accept or reject the transaction accordingly.

This is to ensure that the merchant will not risk the possibility of the customer ending up disputing the transaction. It is the responsibility of the customer to ensure that the merchandise is delivered to his billing address, even if he did not sign for it. This is the reason why many merchants require their customers to register their shipping address as an alternative if different than their billing address. AVS only works in some countries so it does not screen international transactions.

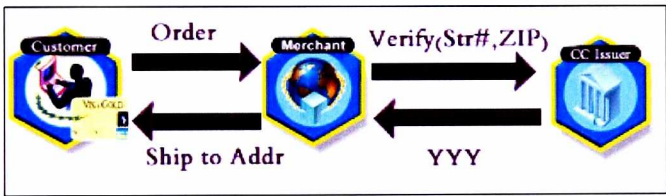


Figure 4-3: Current AVS

Customers fill out an online payment form on the Merchant’s website with their credit card information including the card billing address. The processing network (e.g., FDC, Vital, Nova, GPS, Paymentech) compares the billing address supplied online with the billing address on file at the credit card issuing bank.

From this comparison, the processing network sends an AVS response code to the merchant. Depending upon the response, the merchant may wish to approve the transaction, reject it, or follow other lines of logic. With so many possible reasons as to why an address and zip code may not match, a merchant is not required to refuse a transaction because the AVS response is a mismatch.

The following is a list of possible AVS response codes, and their corresponding meanings. Each code is unique; no AVS response code will ever overlap another in meaning:

A = Address (Street) matches, ZIP does not: This response code signifies a perfect match between the street address entered by the customer and the billing address on file with the card-issuing bank, and a mismatch between zip codes.

B = Address information not provided for AVS check: This response code signifies that the transaction was submitted without address information, so the AVS check could not be performed.

E = AVS error: This response code signifies that an error occurred on the processing network while processing the AVS request, so AVS information is not available for this transaction.

G = Non U.S. Card Issuing Bank: The credit card issuing bank is of non-U.S. origin, and does not support the AVS system.

N = No Match on Address (Street) or ZIP: Neither the street address nor the zip code provided by the customer matches the billing address and zip code on file with the card-issuing bank.

P = AVS not applicable for this transaction: This response code is returned when address information is not checked against the AVS system. Examples of this would be credits, voids, prior authorisation capture transactions, capture only transactions, declines, and other transactions that do not involve address checking.

R = Retry – System unavailable or timed out: VS was unavailable on the processing network, or the processor did not respond.

S = Service not supported by issuer: The issuing bank does not support AVS.

U = Address information is unavailable: Address information is not available for the customer's credit card at the processor.

W = 9 digit ZIP matches, Address (Street) does not: The nine-digit zip code provided matches the billing zip code on file with the issuing bank, and the street address provided does not match.

X = Address (Street) and 9 digit ZIP match: The nine-digit zip code and street address provided match the billing address on file with the issuing bank.

Y = Address (Street) and 5 digit ZIP match: The five-digit zip code and street address provided match the billing address on file with the issuing bank.

Z = 5 digit ZIP matches, Address (Street) does not: The five-digit zip code provided matches the billing zip code on file with the issuing bank, and the street address provided does not match [123].

4.8 Full Address Verification Service FAVS

To re-iterate, fraud in soft-products is an emerging problem. The old solutions that were used for hard-products may not be sufficient for this new type of problem.

Various new ways of detecting and preventing credit card frauds have been proposed, most of these solutions are vendor specific solutions and/or require major modifications on existing e-commerce sites. Often, these solutions are not universal, meaning they are specific to certain credit cards (e.g. Visa, or American Express, but not both) or specific to certain vendors (e.g. Tradecraft). These solutions require customers to download some software (as in Master Card and Discover solutions) or require the bank and merchants to modify their system or checkout procedure (as in Verified by Visa).

So for all soft products MTIO, which require no physical delivery, the merchant is taking the risk by emailing the customer the products. As explained before, this risk is even greater than delivering to a non-billing address for a hard-product, since email tracking is much more difficult comparing to tracking the person living at that address at the time of delivery. Figure 4-4 shows the current situation.

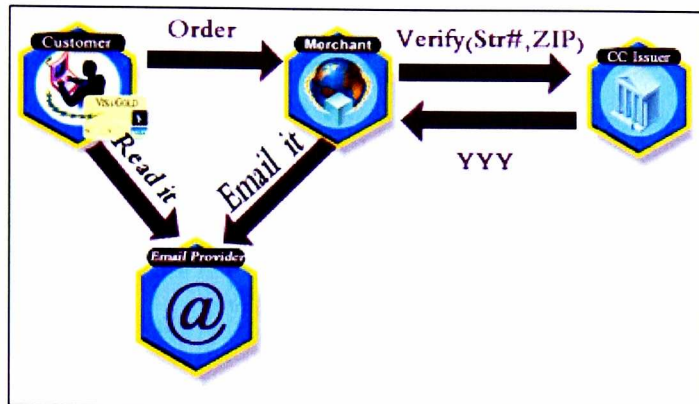


Figure 4-4: Current AVS with Soft Products

In this thesis, improvement of the AVS system is proposed by using the electronic delivery address i.e. email address or mobile number as a verification method (in connection with the billing address). This new system called Full Address Verification System (FAVS)[16] , see Figure 4-5.

In this case, the email address of the customer is stored at his credit card issuer database. When the customer makes an online order for something to be delivered via email the system contacts the bank automatically and compares the two emails: the stored and the supplied emails. This can be performed easily since an email address is not like a name or a street address, which can be written in different way.

It is more effective than matching the billing address since there are no two different emails one for shipping and one for billing. Even if others know the email address in question it will be impossible to access the account (unless by hacking).

Email accounts are unique which makes them easy to be verified. In the case of where the email does not match, the only thing the merchant has to do is to email the customer to send his “trusted” email address or cancel his order.

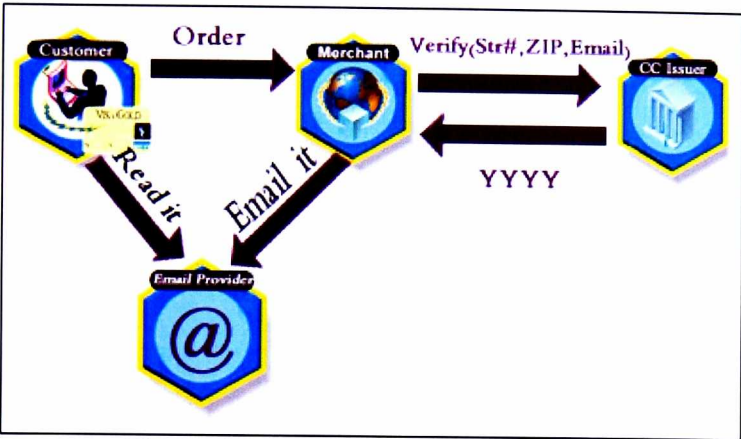


Figure 4-5: Proposed New AVS (FAVS)

4.9 Case Examples: The Problems with Existing Solutions

For the purpose of this thesis two case studies have been conducted into businesses with soft-product e-commerce sites, namely Card4Call [42] and 123CallingCards [1]. Both sites sell prepaid calling cards pin numbers located on the back of normal calling cards. These pin numbers are delivered to customers email addresses where they can use these pin numbers to make international calls from their home telephones. At the same time, interviews with both managing directors revealed that both sites had experienced quite a number of fraudulent transactions and were actively applying automatic and manual fraud prevention methods, such as verifying address, or calling the bank and customer. Table 4-1 and Figure 4-6 show the statistics of fraud transactions occurring with Card4Call. Likewise, Table 4-2 and Figure 4-7 show statistics for 123CallingCards.

Table 4-1: Card4Call Statistics for One Year

System detected frauds	65
Operator detected frauds	104
Undetected frauds	7
Fraud (sum of above)	169
Total Orders	2136
Fraud Percentage	7.9%

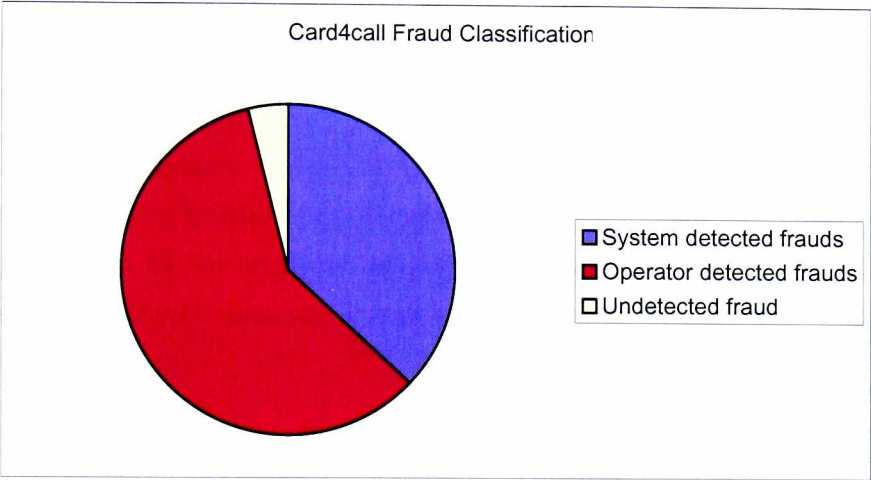


Figure 4-6: Card4Call Statistics for One Year

Table 4-2: 123CallingCards Statistics for One Year

System detected frauds	74
Operator detected frauds	136
Undetected frauds	8
Fraud (sum of above)	210
Total Orders	2124
Fraud Percentage	Around 9.8%

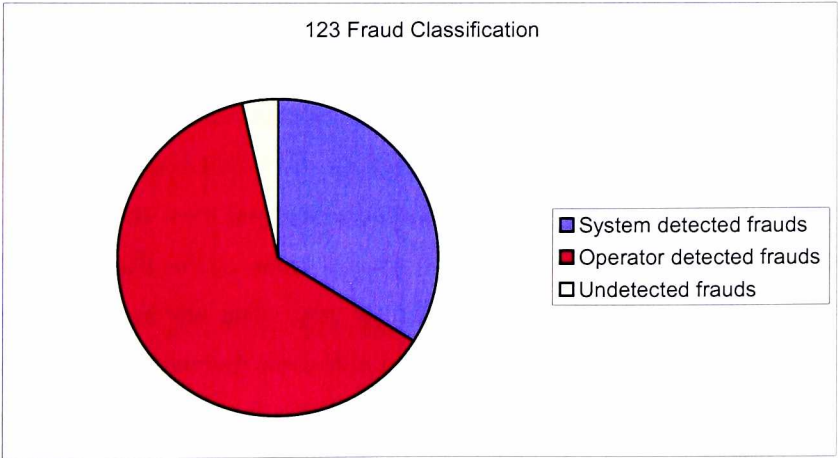


Figure 4-7: 123Callingcards Statistics for One Year

Both Directors agreed that the levels of fraud percentage for their companies were disturbingly high and were costing their businesses considerable amounts in terms of lost turnover.

The detection techniques being used were very time consuming and there were other concerns: pursuing fraudulent transactions invariably led to a trade-off between taking such action and the consequences of processing delays and subsequent costs; from a customer point of view there was also an implied trade-off: between information privacy and shopping online.

The need for personnel within the organisations to call both bank and customer also led to different sets of problems:

Calling banks – a lack of toll free numbers was costly, lack of 24/7 availability was costly, sometimes systems were not available, sometimes banks were not willing to verify customer names and/or phone numbers;

Calling customers – costly again in terms of time and money, customers might not be available and there might be no perfect time to call, the converse of this was that it was often inconvenient for customers if they had to wait for merchant calls.

Significantly, a major concern expressed by both companies was that the types of inconveniences identified and the increasing number of fraud cases were together jeopardizing the mass acceptance of e-commerce, since many customers were becoming increasingly reluctant to shop online.

During the course of the interviews the Company Directors were also asked for their views on the proposed Full Address Verification Service (section 4.8). Their reaction to such a scheme was very favourable and they agreed that if it were to be adopted instead of AVS it would solve most of the fraud cases involving soft products. They acknowledged that the only area in which this would not be effective was that of 'Friendly Fraud'. However since this constituted less than 5% of all fraud cases they felt the shortcoming could be tolerated.

4.10 Fraud Future

It is clear that this is a complicated problem and many soft-products companies are suffering. The major consequence is costly by having to pay higher processing fees and insurance as protection from fraud.

According to the 2004 Mindwave Research report referred to earlier, nine out of ten merchants expected online payment fraud to be the same or worse in 2005, nearly half expect it to be a more serious problem.

Figure 4-8 taken from the report shows the level of concern for merchants and their opinion about the seriousness of the online fraud.

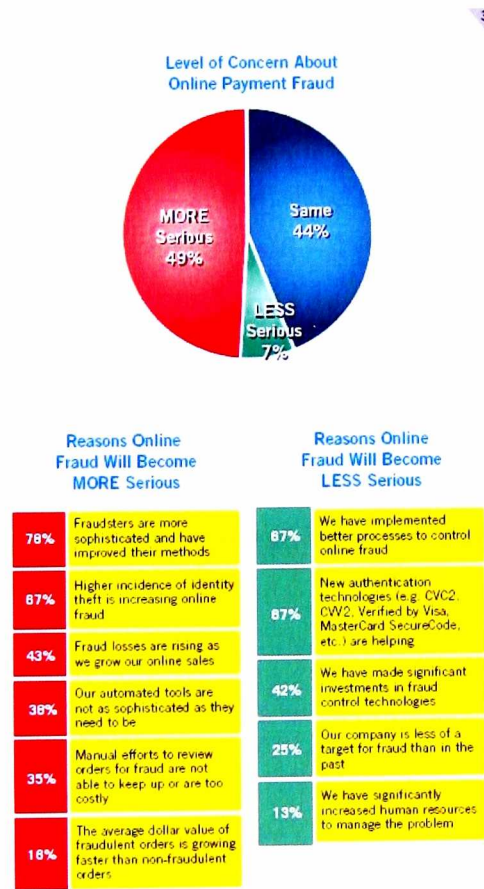


Figure 4-8: Level of Concern about Online Payment Fraud

4.11 Conclusion

The continuing level and implications of fraud in soft products is having serious ramifications for the industry's development. Existing merchants are wary about expansion, and at the same time there is considerable reluctance on the part of potential new entrants regarding start-ups. Unfortunately the current systems, rules and regulations mean that merchants will always be responsible for any fraudulent transaction.

This chapter has provided a critique of current e-commerce fraud prevention and detection techniques. The conclusion it reached was that not all were suitable for e-commerce and therefore complete protection against fraud was not possible.

However, a proposal for improving current state-of-the-art techniques (FAVS) was outlined and reaction from two soft products Company Directors sought. Their views were very favourable although both acknowledged that the new development would not be able to resolve 100% of cases. However since the residue, described by the industry as 'Friendly Frauds' constituted such a small percentage within both the industry and their own businesses, it was not deemed a major issue.

In conclusion, both agreed that if there was industry-wide acceptance of the new proposal, and FAVS is used as a replacement for of AVS the level of fraudulent cases would decrease considerably.

Therefore, having discussed problems associated with current detection and prevention systems, the next chapter intended to present taxonomy of all possible dispute scenarios in the field of e-commerce.

CHAPTER FIVE

Taxonomy of E-commerce

Disputes

CHAPTER FIVE

Taxonomy of E-commerce Disputes

5.1 Introduction

E-commerce now constitutes a significant part of all commercial activity. As a result, there are now many more transactions leading to more disputes. Because of new technology disputes are (i) more frequent, (ii) more technologically complicated and (iii) more difficult in terms of traceability.

Most of the work in the literature has previously concentrated upon the exchange process (involving money and goods), and as a result the focus has only been on problems associated with the exchange process. The problem was one of making sure that the exchange was fair, and concentrated on how to resolve the possibility that one party might receive something but would not send what was promised in exchange. The problem associated with the time of the delivery or the item delivered was rarely studied.

This chapter is intended to present a taxonomy of all possible dispute scenarios in the field of e-commerce. It will analyse scenarios from many different perspectives: computer science, business, legal and also the transaction participants' point of view.

Whilst it is acknowledged that the summary may be subject to improvement in the future, at this moment in time it should provide an adequate basis for Online Dispute Resolution (ODR) systems designers and others dealing with dispute resolutions in order to better understand the nature of the online environment.

Better understanding of situations that might become problematic, how these situations might result in disputes, and the resolution possibilities should provide a useful technical base to achieve better design solutions. Since disputes do not occur in vacuums, and each one arises in a setting or a context, a variety of factors can be affected. For example, the expectations of the parties, the timing of settlement, the perceived urgency of resolution, the consequences of and available alternatives to failure, the role of the third party, and even the form of dispute resolution [19, 80].

All disputes are about one of the three main elements of any transaction: product/service, payment and the exchange of the two. Products and services are almost the same in e-commerce, and these products could be delivered physically like a notebook computer, electronically like a piece of audio or video, or over time such as an Internet or online magazine subscription [19].

Payments in e-commerce are more complicated than normal commerce since in normal commerce nearly all the transactions are conducted using either, cash, cheques, credit cards, debit cards, or wire transfer. In e-commerce, whilst all the above are applicable many other new payment systems, e.g. E-cash, E-coin, Paypal now exist. Complications arise from the introduction of new payment systems, frequently making the new payment systems take a long time to become established. In contrast the original five methods cited are tried and tested.

Exchange of goods and payment in e-commerce is also a major contributor to the causes of disputes since the exchange may take more than one form depending on the product purchased and the payment method used.

In the following sections dispute cases will be studied in general and will not specifically be concerned about any goods, payment or exchange method. Therefore, if the credit card is not valid the dispute reason will only be described as “payment quality is not good” and will not consider any other reason, e.g. whether it had expired, was not yet valid, whether the expiry date did not match or it had been stolen.

The remainder of the chapter will then give a brief definition of the term ‘dispute’, list the assumptions, notations and the transaction elements used to clarify the taxonomy of dispute. All possible dispute cases will be formally listed using the 'Truth Table' approach, and a comprehensive taxonomy framework for dispute in e-commerce will be derived from these possibilities. The chapter will conclude by discussing possible directions for future research in this area.

5.2 Disputes

Disputes and complaints are two words that are frequently being used interchangeably without providing any definition or context. However, there are various types of damaging or injurious experiences that consumers may have. Commentators often refer to a 'pyramid of injurious experience' or a 'dispute pyramid' see Figure 5-1 [66]. At the base of the pyramid is unperceived injurious experience, moving up to perceived harms, grievances and complaints. At the very top of the pyramid, forming the smallest category, are disputes with a subset being disputes voiced to third parties and pursued through formal dispute resolution that would include Alternative Dispute Resolution (ADR) as well as lawsuits.



Figure 5-1: The Dispute Pyramid

The layers of the dispute pyramid have been characterized in the following manner [11]:

Unperceived injurious experience: where consumers may experience a problem with a transaction but never perceive it as injurious per se. For example, a consumer may lack

the expertise to recognize a specific problem such as a product defect that makes a product work inefficiently.

Perceived injurious experience: out of the larger mass of experience, some of it is perceived by individuals as injurious. A consumer or customer, however, may blame him or herself or feel that the injury is too vague or debatable to be susceptible to a remedy. Thus, the experience may never develop into a grievance.

Grievances: it is a sense of violation of a right or entitlement that can be ascribed to a specific person or entity. Grievances are usually not voiced, although they may make customers decide not to return to a particular merchant or type of merchant or medium. For example, a consumer who has a grievance arising out of an Internet transaction may choose never to use the Internet for future purchases. When a grievance is not voiced the consumer, in essence, absorbs the loss.

Complaints or claims (not legal claims or complaints): a complaint is a grievance that is voiced to the perceived offending party. Most frequently, complaints are granted or redressed. These would be referred to as “resolved” complaints. Reputable merchants, who seek repeat business and value positive reputation among consumers will encourage customers who perceive grievances to complain. A merchant who receives a complaint is in a position to grant relief and to satisfy the customer. Granting relief builds trust and confidence with the customer for future dealings.

Disputes: a dispute, as contrasted with a complaint, is a complaint that has been rejected in whole or in part. Often, customers do nothing after a complaint has been rejected by a merchant. This is another stage at which consumers may choose to absorb or internalize the loss. This is often rational because the cost of pursuing relief may be more expensive than the loss itself. The customer, however, may choose to avoid future dealing with the merchant and can create negative feedback or word of mouth.

Disputes voiced to a third party. A small fraction of customers with disputes choose not to give up but to seek the assistance of some third party. Third parties might include a government agency, a merchant association or a lawyer ombudsman. Quite often, the

third party will advise a consumer that it is not worth it to commence a formal proceeding against a merchant.

Formal dispute resolution would include ADR or lawsuits. This is the top of the pyramid and the smallest category on the dispute pyramid.

Since this thesis focuses on disputes in general the rest of this section will concentrate on discussing the possible causes of disputes.

5.3 Assumptions, Notations, Transaction Elements

5.3.1 Assumptions

In this section some of the assumptions which will make it easier to give a clear and general taxonomy for E-commerce disputes are as follows:

A1: a payment is a payment regardless of its form;

A2: a payment is actually a special item that a Party wants to exchange with another party for another item - which might be payment too;

A3: disputes will only occur after one of the two parties involved in the transaction delivers the item;

A4: if an item was delivered to the wrong address or could not be delivered because a wrong address was supplied, it will be considered that the item had been delivered but that the delivery address was incorrect (since the sender already attempted to send it).

A5: each transaction will have two different parties P_x and P_y , so X and Y can be used interchangeably.

5.3.2 Notations

The notations used in this chapter and that will be used in any forthcoming chapters are as follow:

P_x : Party x who wants to exchange something with Party P_y .

I_x: Item that P_x wants to exchange.

Q_x: Quality of the item I_x.

C_x: Number of Items I_x that P_x wants to exchange in a single transaction.

A_x: Delivery Address of P_x.

T_x: Time interval where P_x will expect P_y to deliver within.

D_x: Actual Delivery of I_x by P_x to P_y

S_x: Satisfaction level P_x promises P_y

M_x: Consumption of I_x by P_y

5.3.3 Transaction Elements

Each transaction has eighteen elements that constitute the contract:

(P_x, I_x, Q_x, C_x, A_x, T_x, D_x, S_x, M_x) and (P_y, I_y, Q_y, C_y, A_y, T_y, D_y, S_y, M_y)

Any E-commerce transaction will go through the following three steps

- Order and Negotiation

In this stage P_x and P_y will negotiate and agree on the following:

(P_x, I_x, Q_x, C_x, A_x, T_x) and (P_y, I_y, Q_y, C_y, A_y, T_y)

- Actual Exchange

In this stage D_x and D_y will take place

- Post Transaction

In this stage both P_x and P_y can generate (S_x, M_x) and (S_y, M_y) respectively.

5.4 Dispute Definition

As a result of the literature survey (which reviewed the nature and causes of disputes) and problems that were specifically associated with e-commerce, it is important to give further consideration to this overriding concept and its implications since it is central to

the whole thesis. This section offers a series of definitions which are progressively refined as significant questions are posed that challenge each stage and culminates in what is viewed as the optimum.

Def.1: The two parties involved in the transaction disagree on one of these elements after that transaction is completed.

But what: if dispute happened before the transaction is completed for example when one party sends his item but the other doesn't?

Def.2: The two parties involved in the transaction disagree on one of these elements after at least one party delivers his item to the other.

But what: if dispute happened in more than one element?

Def.3: The two parties involved in the transaction disagree on one or more of these elements after at least one party delivers his item to the other.

But what : if one steals a payment method and uses it in a transaction; the disputant will not be part of the transaction since they only use his payment method and may or may not consume the other item.

Def.4: The two parties whose item is exchanged or will be exchanged in the transaction disagree on one or more of these elements after at least one party delivers his item to the other.

But what : does Disagree mean?

Def.5: One or both parties whose item is exchanged or will be exchanged in the transaction do(es) not meet the agreed contract terms.

But what : if one of them does not meet the agreed terms but the other does not complain.

Def.6: One or both parties whose item is exchanged or will be exchanged in the transaction do(es) not meet the agreed contract terms and the affected party is complaining.

This will be the definition of dispute which will be used for the rest of this thesis.

5.5 Proof of Completeness

In order to make sure that all the possible dispute cases are covered, the Truth Table for it should be generated and all the possibilities are studied.

Each party involved in the transaction has nine attributes (Px, Ix, Qx, Cx, Ax, Tx, Dx, Sx, Mx) and since the study is about transactions between two parties, eighteen attributes- nine for each- will be used to generate the Table.

Each attribute will take the value of True or False if the desired action was completed successfully or unsuccessfully respectively (e.g. Ix is true if the party involved in the transaction Px agrees that Ix is the item he ordered and it will be false if he claims that Ix is not what he ordered) and so on for the rest of the attributes.

Eighteen features mean that the size of the table will be $2^{18} = 262144$ Tuples.

Since it is quite long and time consuming to generate the whole table, minimization as much as possible without sacrificing any aspect of the truth table was performed.

The table will have all the eighteen features and a ‘Success’ result which is the ‘AND’ of all the features. Sequence (ordering) of features in the table will not affect the result since it is Anding.

‘Success’ means that the transaction will be completed with no disputes.

‘?’ means that at this stage it is not possible to decide if the transaction will end with no dispute or not.

The start will be with the actual delivery D since it is a critical feature

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T																	?
T	F																	NO
F	T																	NO
F	F																	YES

From the table above if either of the two parties involved deliver and the other does not (T F or F T) then the success will be “NO” meaning that there is no hope for this transaction to be successful since one party will surely dispute. This means that 50% of the possibilities are guaranteed disputes.

If both (D_A and D_B) are FALSE then success should be “NO” but as an exception and according to assumption A3 it will be “YES” meaning that there could be no possible disputes at all since no exchange has happened. This will eliminate 25% of the table making only the remaining 25% unsure in terms of possible success.

131072 possibilities are disputes regardless of the others which means (D_A or D_B) and 65536 are successful transactions since (¬D_A and ¬D_B).

The table now has 262144 – 131072 – 65536 = 65536 possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T															?
T	T	T	F															NO
T	T	F	T															NO
T	T	F	F															NO

Now if either of the two parties or both deny participating, it will result in a dispute. From the 65536, 75% are disputes regardless of the rest which means (P_A) or (P_B) is FALSE

The table now has 65536- 49152=16384 possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T	T	T													?
T	T	T	T	T	F													NO
T	T	T	T	F	T													NO
T	T	T	T	F	F													NO

If either of the two parties or both claims that the item received is not what he agree with the other, it will also result in a dispute. From the 16384, 12288 are disputes regardless of the rest which means (I_A) or (I_B) is FALSE.

The table now has $16384 - 12288 = 4096$ possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T	T	T	T	T											?
T	T	T	T	T	T	T	F											NO
T	T	T	T	T	T	F	T											NO
T	T	T	T	T	T	F	F											NO

From the 4096, also 75% are disputes regardless of the rest which means if (Q_A) or (Q_B) is FALSE (i.e., either of the two parties or both claim that the quality of the item received is not what both agreed on) it will result in a dispute.

The table now has $4096 - 3072 = 1024$ possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T	T	T	T	T	T	T									?
T	T	T	T	T	T	T	T	T	F									NO
T	T	T	T	T	T	T	T	F	T									NO
T	T	T	T	T	T	T	T	F	F									NO

From the 1024, 768 are disputes regardless of the rest which means if (C_A) or (C_B) is FALSE (i.e., either of the two parties or both claim that the quantity of items received is not what they agreed on) it will result in a dispute.

The table now has $1024 - 768 = 256$ more possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T	T	T	T	T	T	T	T	T							?
T	T	T	T	T	T	T	T	T	T	T	F							NO
T	T	T	T	T	T	T	T	T	T	F	T							NO
T	T	T	T	T	T	T	T	T	T	F	F							NO

From the 256, 192 are disputes regardless of the rest which means if (A_A) or (A_B) is FALSE (i.e., either of the two parties or both claim that the delivery address of the other party is not correct and that why the item was not delivered to him) it will result in disputes

The table now has $256 - 192 = 64$ possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T	T	T	T	T	T	T	T	T	T	T					?
T	T	T	T	T	T	T	T	T	T	T	T	T	F					NO
T	T	T	T	T	T	T	T	T	T	T	T	F	T					NO
T	T	T	T	T	T	T	T	T	T	T	T	F	F					NO

Out of the 64, 48 are disputes regardless of the rest which means if (T_A) or (T_B) is FALSE (i.e., either of the two parties or both claim that the item he expect does not arrive on the time agreed) it will result in a dispute.

The table now has $64 - 48 = 16$ possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T			?
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F			NO
T	T	T	T	T	T	T	T	T	T	T	T	T	T	F	T			NO
T	T	T	T	T	T	T	T	T	T	T	T	T	T	F	F			NO

Out of the 16, 12 are found to be disputes regardless of the rest which means if (S_A) or (S_B) is FALSE (either of the two parties or both claim that he is not satisfied with the item received) it will result in a dispute.

The table now has only 4 possibilities to check

D _A	D _B	P _A	P _B	I _A	I _B	Q _A	Q _B	C _A	C _B	A _A	A _B	T _A	T _B	S _A	S _B	M _A	M _B	Success
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	Yes
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F	NO
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F	T	NO
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F	F	NO

Out of the 4, 3 are disputes regardless of the rest which means if (M_A) or (M_B) is FALSE (i.e., either of the two parties or both claim that the other one consume his item more than what they agreed on) it will result in a dispute.

So the table end up with 1 case with no dispute which is when all the values are True.

The success formula will be

Success = $\{(\neg D_x \& \neg D_y) \text{ or } ((D_x \& D_y) \& P_x \& P_y \& I_x \& I_y \& Q_x \& Q_y \& C_x \& C_y \& A_x \& A_y \& T_x \& T_y \& S_x \& S_y \& M_x \& M_y)\}$ where x and y belongs to $\{a, b\}$ and x not equal y

Dispute formula should be \neg success which means Dispute transaction will be:

DT= $\{ (D_x \text{ xor } D_y) \text{ or } \neg P_x \text{ or } \neg P_y \text{ or } \neg I_x \text{ or } \neg I_y \text{ or } \neg Q_x \text{ or } \neg Q_y \text{ or } \neg C_x \text{ or } \neg C_y \text{ or } \neg A_x \text{ or } \neg A_y \text{ or } \neg T_x \text{ or } \neg T_y \text{ or } \neg S_x \text{ or } \neg S_y \text{ or } \neg M_x \text{ or } \neg M_y\}$ where x and y belongs to $\{a, b\}$ and x not equal y

5.6 The Taxonomy

In this section all the possible dispute causes will be listed on the basis of the primary research that has been analysed earlier in this chapter.

There are two important points to clarify: first, in any transaction there could be more than one dispute case because one party will dispute and then the other will dispute the dispute and so on, until a final dispute resolution is achieved. In this classification each dispute is considered a case and treated separately.

Second, in any dispute case there could be more than one cause. In this classification the concentration is on the causes, so each cause will be treated as a separate dispute case [16, 35, 52, 84, 124, 141].

The assumption here is that Party X wants to buy something from Party Y.

The following is the taxonomy that has been derived from the complete definition of the Dispute Formula's elements.

(For ease of understanding and referring to dispute cases, it has been broken down into three major headings. In turn each of these headings is then defined as a series of sub-headings with appropriate descriptions of each element of the relevant dispute formula):

1. Delivery: Here all dispute reasons that caused by a problem of delivery are gathered

a. Payment received but goods not delivered ($Dx \ \& \ \neg Dy$)

This is a clear case and no need for more clarification.

b. Goods received but payment not delivered ($Dy \ \& \ \neg Dx$)

This is also clear case and no need for more clarification.

c. Goods not delivered on time ($\neg Tx$)

In this type a dispute may occur because the goods were not delivered on time. E-tickets have no value after the flight time, so if an e-ticket received late then this is a good reason to dispute the transaction.

d. Payment not delivered on time ($\neg Ty$)

In this type a dispute may arise because the payment was not delivered on time. Late payment may result in financial penalty on the merchant and he may have to pay an interest in such cases, so if the payment is received late, this would be a good reason to dispute the transaction.

e. Goods can not be delivered ($\neg Ax$)

In this type the goods cannot be delivered for some reason that has been caused by the customer, for example, a wrong address or and invalid email. If goods cannot be delivered because of the merchant then this is Dispute{1-a} above and the reason for non-delivery is not important.

Disputes may arise from both sides, the customer could claim he never received the goods and asked for a credit to what was paid. However this is not considered here because it is the same dispute as Dispute{1-a}. The merchant might dispute because crediting a customer could mean a chargeback for which he will have to pay a fee (and it could also be considered as bad credit for his merchant account). So his dispute could claim that the customer caused the mistake by providing the wrong delivery address, and

if any was payable then it should be the customer's responsibility. In this case the merchant would have good reason for the dispute.

f. Payment can not be delivered ($\neg A\gamma$)

In this type the payment can not be delivered for reasons caused by the merchant e.g. a wrong account number or revoked key. If payment cannot be delivered because of the customer then this is Dispute{1-b} above. Dispute may be caused by both parties, the merchant may claim he never received the payment and may ask for his goods to be returned at the customer's expense or for the late payment penalty to be made by the customer and not himself. However this is not considered here because it is the same dispute as Dispute{1-b}. The customer may file a dispute claiming that he should not be held responsible for returning the goods or making the penalty payment since it would constitute extra expense and the fault was the merchant's for providing a wrong account number, therefore any fee should be paid by the merchant. In this case the customer would have a good reason to create a dispute.

2. Order: This is a compilation of all of all dispute reasons connected with the order or the transaction itself.

a. Customer claims never placing the order ($\neg Px$)

In this type of dispute the customer is charged for a transaction and he claims that he never placed it, whether the goods were delivered or not is not part of the issue, what matters is whether or not the order was placed.

b. Merchant claims no order made ($\neg Py$)

In this type of dispute the merchant is held responsible for a transaction but claims that he never received it. Whether payment was or was not delivered is not the issue, what is of concern is whether or not the merchant received the order. A possible scenario is a customer who is buying an E-ticket, if the customer loses any money because of the merchant not delivering the E-tickets and the customer subsequently wants compensation, this could be part of Dispute{1-b}, then the merchant will dispute this saying that he never received such an order.

c. Order quantity is not correct ($\neg Cx$)

In this type both the customer and the merchant may dispute things by claiming the quantity ordered was respectively less or more than what was ordered.

d. Amount paid incorrect ($\neg Cx$)

In this type both the customer and the merchant may make a dispute by claiming that the payment amount was respectively more or less than the value of what has been ordered.

3. Item: Here all dispute reasons that caused by a problem regarding the exchanged items are gathered

a. Received goods not as purchased ($\neg Ix$)

This is a common dispute reason where the customer ordered something and then received something completely different. A straight forward example might be when a customer ordered a video about the World War I and received a video about The World Cup.

b. Received money not as sold ($\neg Ix$)

This usually happens when transactions are conducted between cross border parties, the merchant approves an order worth of 200 Pounds and the customer transfers 200 US Dollars. There should be a distinction here between this type and Dispute{2-d} because here the customer is claiming that he is purchasing something worth 200 US Dollars while in Dispute{2-d} there is no disagreement on the price but the customer is paying less than what has agreed for whatever reason.

c. Quality of Received goods not as promised ($\neg Qx$)

In this type the customer disputes a transaction because he claims that what he has been promised has not been delivered. For example, if it is something physical it could be damaged or if a video file, it could have bad picture or other quality problems.

d. Money quality not proper ($\neg Qx$)

In this type the merchant disputes a transaction because he claims that what he has been promised as payment has not been delivered. It could be in the form of counterfeit money, an expired credit card, or any other payment quality problem.

e. Received goods not as expected ($\neg Sx$)

This type of dispute is considered one of the hardest to resolve since satisfaction cannot be measured. The customer will claim that what he received was not what was expected when placing the order.

f. Received money not as expected ($\neg Sx$)

The merchant will claim that what he received as payment is not what was expected when approving the order.

g. Multiple payment consumption ($\neg Mx$)

This could happen because of using different payment methods at the same time, for example, paying by a credit card and because it was not approved on time then another payment method is used, for example a cheque. After the cheque has been processed, approval for the credit card transaction might subsequently arrive. This type of situation might also arise due to the use of a self approved payment method such as a credit card where the merchant can charge a card without the approval of the customer, or e-cash is used where the customer only signs the e-cash with his private key but there is nothing to stop the merchant from submitting the e-cash more than once. Whilst there are other possible reasons, the major concern here is on the multiple charging from the point of view of the consumer.

h. Multiple Goods consumption ($\neg My$)

This type of dispute is rare but still possible. One example is where a customer might order one notebook but the merchant sends two notebooks against the same order but only charges the customer once, also in pay-per-view movies a customer may watch the movie twice and be charged only once.

5.7 Conclusion

Using electronic means to do business can greatly improve the efficiency of the business transactions. However it creates some problems that were not previously considered important. One class of problems results from the behaviour of untrustworthy participants; as a result of reasons such as dishonesty and network failure, disputes may arise. Online alternative dispute resolutions (online-ADR or ODR) have been heavily researched but none have tried to identify the reasons behind disputes to then be able to provide a complete ODR solution

In this chapter, disputes were classified according to all the factors of the transaction in which the disputes arose. The intention was to begin to provide software designers and others involved in the dispute resolution process with an appropriate framework to begin to work towards achieving optimum understanding and, eventually, solution.

To this end, it has been necessary to first of all classify these disputes according to their causes and then go on to provide a formal method of proving the validity of the results (via the Truth Table format).

This work has proposed the first taxonomy for dispute cases in e-commerce. The taxonomy was created using actual case study evidence and personal experience in this field. The intention was that the taxonomy generated would be general (in the sense that it could apply to any payment method used or product purchased).

Whilst instances may be found where this taxonomy might not seem to apply because it does not define their particular reason for dispute (e.g. where a customer might write a cheque and not have enough in a bank account to cover the amount), closer analysis of the taxonomy will reveal that the analysis is robust in every situation. In this particular situation, category (3-d) Money quality not proper ($\neg Qx$) could be used to explain it.

Due to time constraints this work has been limited by a number of assumptions (see 5.3.1). Future work should try to study each reason separately in order to minimize these assumptions as much as possible. At the same time the intention has been to provide more detailed proposals as to solutions for prevention or resolution of the conflict.

Next chapter will study current Online Dispute Resolution (ODR) systems and their suitability for the e-commercial world in more detail and check if any can resolve all the taxonomy disputes cases.

CHAPTER SIX

Online Dispute Resolution

CHAPTER SIX

Online Dispute Resolution

6.1 Introduction

Online Dispute Resolution (ODR) can have several meanings, however in this thesis it is defined as the online technology applied to alternative dispute resolution. The term Alternative Dispute Resolution (ADR) means dispute resolution other than litigation in the courts, and includes arbitration. In the real world ADR systems are being used quite successfully as effective, quick and efficient methods of dealing with consumer complaints that are not resolved through simple contact with the other party [75].

However, with the growth of e-commerce and therefore an inherent growth in the number of dispute cases, there is already evidence of an increasing number of successful online dispute resolutions (ODRs), relating to business-to-consumer Internet transactions. In these situations ODR can address consumer concerns fairly and appropriately, allowing both parties to avoid the delays and the costs of appealing to either a government administrative agency or the courts. Additionally, it lowers pressures on administrative and judicial systems but at the same time manages to preserve the consumer rights to seek legal redress should they be dissatisfied with the results of the ODR process.

One major advantage of ODR is the ability to find more flexible and creative solutions that satisfy both parties, (whereas consumer protection agencies and/or courts may offer only limited remedies in resolving disputes, particularly where they are prescribed by law or regulations)[56]. Therefore ODR's potential for managing e-commerce conflict remains strong because of its fit with soft-products and its particular advantage over traditional legal mechanisms [101].

A second important advantage relates to its cost-effectiveness: E-commerce by its very nature has resulted in an increasing number of long distance (and cross-border) interactions. Therefore, disputes can be between parties who are located far from each other. Litigating and enforcing such disputes through the courts can be disproportionately expensive for smaller and medium-size claims due to added costs (such as employing

local lawyers, travel and translation costs). The implication here is that only redress for very large claims can be obtained in this way.

However, the value of most e-commerce transactions undertaken by consumers at the moment is very small, covering items such as books, music, software and other consumer goods, although this may change in the future if consumers feel confident about buying higher value goods such as cars or financial services over the Internet.

For the time being at least, the general cost of legal redress by litigation for e-commerce disputes is therefore not proportionate to the value of the claim. As a result, for such claims, cost-effective Online Dispute Resolution (ODR) schemes seem to be the only viable means of redress. For all parties concerned it is essential that this system proves trustworthy and effective in the long term since a lack of trust in this area of redress may mean that consumers will not engage in e-commerce and will affect the growth of the whole industry.

Another significant problem related to cross-border transactions is the difficulty of determining the appropriate forum for resolution since there will be an inevitable conflict between the forum of the claimant and the respondent. Being located in no particular geographical area, ODR mechanisms can provide a forum equally convenient and accessible to either party [73].

Choosing the “country of origin” as the applicable law alone may not be sufficient to boost trust in online transactions, because consumers are unlikely to be able to reach courts in other countries where merchants are resident for many obvious reasons. Similarly, choosing the “country of destination” which is the country of the customer is not the right choice either. Merchants will not be eager to conduct international transactions that could lead them to a mixture of laws depending on where the customer may live. In addition, even if customers agree to the law of the merchant's country or vice versa, most of the time the cost of pursuing the case will be much more than the price of the item in dispute because of the cross border expenses and the low value of most e-commerce items.

ODR can be offered in different approaches, the most widely known three are “arbitration”, “mediation” and “conciliation/negotiation”. These three are often used interchangeably and without much precision but the role of the dispute resolver in the process and the degree of enforceability of the results make the distinction [56].

This chapter will study current ODR systems and their suitability for the e-commercial world in more detail. It will conclude by suggesting that not all methods are suitable for e-commerce transactions with soft products, since in most situations there will be a human element involved in the resolution process, automatically adding more cost. (The average cost of an e-commerce transaction is less than £20, most ODR providers ask for more than this to resolve a dispute).

6.2 Necessity for ODR

The need for ODR is clear. Perritt in [107] claims that “three characteristics of the Internet make traditional dispute resolution through administrative agency and judicial procedure unsatisfactory for many controversies that arise in Internet-based commerce and political interaction.”

- “The Internet’s low barrier to entry invites participation in commerce and politics by small entities and individuals who cannot afford direct participation in many traditional market and political arenas.”
- “The geographic openness of electronic commerce makes stranger-to-stranger transactions more likely.”
- “the Internet is inherently global” .

In addition, since E-commerce is relatively new it may not yet be covered or described well in law’s various forms, e.g. cases, codes, and commentary [101]. Furthermore, disputes in online transactions with cross-border participants and especially low value transactions, are best resolved by ODR because of its convenience. Participants do not

have to move while the dispute is in resolution stage since they can follow up using their own PC's.

The choice of going to court in disputes resulting from international Internet transactions is complicated by complex questions such as 'What is the applicable law?' and 'Who has jurisdiction over such disputes?' Moreover, international court proceedings can be very expensive, most of the time higher than the value of the goods or services in dispute. If going to court was the only choice E-commerce customers had in order to resolve any dispute regardless of its nature then consumer and merchant confidence would decline. Customers and merchants would then restrict their choices to the scope of their geographic area, which would not only limit competition and consumer choice, it would also invalidate one of the main advantages of using the Internet.

For many reasons, most online disputes are resolved via informal methods such as direct negotiation; however, some conflicts require more formal responses and ODR is also now part of that formal response. It shares dispute resolution responsibilities with 'positive' law, as well as filling gaps where the law is unable to help. As a mechanism that perfectly fits online conflicts, ODR has become the default for managing certain forms where both dispute and resolution are conducted online. ODR has many advantages over traditional resolutions, for example, cost, the ability to deliver dispute resolution expertise at a distance, and the ease of settling disputes from the comfort of a personal computer [101].

Businesses that show they have managed customer service and internal complaint handling systems will provide a measure of assurance to consumers that they are abiding by some acknowledged standard of service or reliability. These types of businesses would therefore argue that providing this kind of customer service implies they are not likely to have to be involved in any ODR case. In this way they can ensure a constant market share in their business sphere, hopefully reducing the likelihood of costly, cross-border legal battles. Investment in such systems should also improve customer perceptions of their image and provide valuable feedback to help expand and improve their business activities [102].

In terms of consumer confidence, ODR can be initiated irrespective of whether the business has offered it or not. Although consumers have the right to legal redress in their own countries, more often than not ODR is perceived to be more attractive since the expense, time, complexity and uncertainty of judicial processes can make court action impractical for such small transaction amounts. Cross-border scenarios also compound the problem with issues such as jurisdiction, applicable law and enforcement difficulties [102].

Finally, another factor making ODR in e-commerce disputes an important issue is the unequal bargaining power of customers when compared to the merchant. A balancing of unequal bargaining power is particularly necessary where the supplier relies on standard terms and conditions and where, as is usually the case, suppliers need consumers to pay in advance for the transaction. For this reason there are many instances where the claimant will be the consumer who is not usually willing and may not have enough finance to be able to go to court. To this extent ODR can provide an affordable and effective dispute resolution mechanism and it may contribute to achieving the aim of creating trust in e-commerce and practical redress for consumers [75].

6.3 Nature of ODR

To re-iterate, if an ADR process is implemented using web based information management and communication and in some cases database applications, then it is described as an ODR. ODR requires its users to access sites and submit or download information from the Internet and due to the relatively rapid growth of networked information technology it has the potential to dramatically increase access to conflict management by many who would otherwise forego third party facilitation.

Whether litigation or ADR, there are physical variables to be addressed which ODR transcends [79]. It can now reach into homes, offices, schools and Government worldwide, making it more accessible and preferred by customers and merchants alike. However, it does present other obstacles, most significantly the need for networked

information technology. At the same time some Internet users may not be experienced enough to make it work to maximum effectiveness.

ODR is sometimes described as a “Fourth Party,” supplementing traditional ADR third party facilitators or neutrals that in the past have been deemed critical to resolving disputes outside of traditional litigation [80]. Its main application is with particular resolution models such as mediation, arbitration, and negotiation.

There are two basic ODR approaches: Dispute Avoidance (DA) and Dispute Resolution (DR). Dispute Avoidance is informal ODR, where IT is used to help prevent complicated disputes from arising, minimizing the need for formal resolution or other DR approaches. It benefits from the fact that online transactions, regardless of social setting or context, are considerably less robust than offline transactions [101].

The main DA technologies include credit card ‘chargebacks’ and online money transfer, or escrow services. These facilitate a wide range of online transactions from marketplaces such as LLBean.com to auction sites such as eBay[58]. The chargeback system allows credit card companies such as Visa and American Express to credit customers with what has been debited from their account. This is likely to happen when customers are not able to get satisfaction from merchants for a charge they are either unwilling to accept or unable to recognize. More people prefer to use credit cards in e-commerce transactions because of this facility since financial liability is largely removed from them and is transferred to the merchant and as a result the benefit of the doubt is in the consumer’s favour [101].

New online payment systems are relatively simple and help reduce some of the costs associated with previous systems such as waiting for money orders to arrive via snail mail or transferring payment before delivery of the item. Online third party payment systems, e.g. Paypal [106], maintain personal accounts similar to banking systems. Users can add money to their accounts via credit cards, cheques, money orders or electronic fund transfers.

However these new systems are not regulated or insured in the same way as banks. Users do not use their accounts to conduct transactions directly, in the case of Paypal they will

have to ask for payment for a transaction after being notified that it has been requested and authorized. Paypal will then debit a credit card or a current account, authorize a cheque or adjust an interest earning balance for a users accounts. In spite of the apparent hurdles, these new online systems will still help the use of ODR in DA.

Feedback or Rating is another DA mechanism which will provide customers and merchants with information profiles gathered from data about previous transaction related behavior. These profiles provide a track record or reputation rating that can help both customers and merchants when making decisions about whether or not to proceed with the transaction. One good example of such a service is the eBay feedback rating system where both buyers and sellers are ranked by those they do business with. E-Bay then computes overall positive and negative ratings upon which decisions to trade in the future may be tied.

Another important DA mechanism is the Trustmark, also called Trustseal. This is a kind of hallmark that acts as an indicator of good practice for the processes involved in online commercial activity, the inherent need for privacy and trust in dispute resolution procedures. Online services or enterprises pay for the mark or seal to appear on their site to verify accreditation and achievement of pre-defined standards. If the seal appears in their site this means that they adhere to the stipulated standards and are therefore accredited by a trustmark or trustseal service provider, e.g. TrustE [134] and SquareTrade [126]. These signs of accreditation are important to the ODR process since they help prevent disputes from arising in the first place and because they stipulate recognized standards of dispute resolution [101].

6.4 Development of ODR from ADR

6.4.1 The Development of ADR

Alternative Dispute Resolution (ADR) was established in the latter half of the 20th Century [30]. Disputes are resolved outside the courts using professional practices and theories. They are not usually binding and participation is largely voluntary, comprising

direct or facilitated negotiation. Mediation is usually by a neutral third party and for each case they will have different levels of power in terms of structuring the exchange and finding a solution. Since litigation is time consuming and costly it acts as a powerful disincentive to adversarial dispute resolution. These concerns led to ADR's development and ultimate acceptance [65]. ADR established a remedy called win-win solutions, and benefited from cost advantage.

Although for most of the time ADR is not a binding force, arbitration can be binding and is recognized as law through statutes such as the U.S. Federal Arbitration Act (9 USCS 1), The U.K. Chartered Institute of Arbitrators [26], and transnational conventions such as The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards [85, 101].

A major feature of ADR is the shift of control in dispute resolution from courts to the parties who are directly involved in the dispute. In addition the outcome of the resolution is usually satisfactory for both [all] participants.

“ADR has proven that moving justice away from the courthouse is often desirable and that the arena of dispute resolution, once thought to be the exclusive domain of law and courts, is markedly different from what it was several decades ago. Mediation arbitration, and other forms of ‘alternative’ dispute resolution are now the most common approaches to dealing with conflict”[80].

6.4.2 Subsequent Development of ODR

ODR systems did not emerge until the World Wide Web became ubiquitous in the mid 1990s. The Internet helped boost and encourage e-commerce, and as a result disputes start to arise, leading many people to think that the only way to resolve online problems would be to use online dispute resolution. The collapse of the “Dot Coms” in 2000-01 had a dramatic impact on ODR. As a result the impetus for developing ODR was declining. Nevertheless certain areas were still active, in particular those involved in resolving disputes relating to online auctions, insurance claims and domain names [101].

The first experiments in extra-judicial ODR were made during 1996/1997 in the US and Canada [76]. Having begun as university projects, they eventually evolved into commercial ventures. By way of contrast, European Governments and most notably the European Commission were strongly advocating the use of ODR systems for consumer disputes around the same time [116]. By the early 2000s a considerable amount of private entrepreneurial activity had developed: in 2002, 30 consumer ODR schemes were recorded [75].

Before 1995 no universal online standard existed. With the development of faster and more efficient Internet connection and other features such as HTML editors and browsers, ODR very quickly gained mass acceptance. However, with its growth came the consequence of more conflict. Virtual Magistrate online arbitration system was established in the same year through which ISP disputes could be handled [109].

Virtual Magistrate, and later the Online Ombuds was developed at the University of Massachusetts, along with the Family Mediation Project at the University of Maryland. These were both implemented with support from the National Center for Automated Information Research. Although the Initiator for all of this was a rise in the number of disputes, the real aim was to refine the use of information technology in dispute resolution as a whole.

ODR's second developmental period was dominated by two trends, the rapid proliferation of online activity and technologies to support it, and the emergence of ODR prototypes from academic institutions. Whilst around 1995 academic sponsored prototypes dominated, by 1998 almost 50 private entrepreneurial offerings had been developed [101].

As an important part of the process, businesses involved in ADR worked with those in the Internet to produce online versions of offline ADR practices, since it was felt that IT could be used to improve the provision of non-adversarial resolutions regardless of context.

6.5 ODR and E-commerce

The growth of e-commerce has produced disputes between businesses (B2B), businesses and consumers (B2C), and between consumers (C2C). These disputes vary greatly in terms of value, location, and rule structures. E-commerce disputes can happen for many of the same reasons as offline commercial disputes, e.g. one side of a transaction might not be satisfied with what has been purchased or the way the item has been delivered and will be looking for some kind of compensation as a result [119].

In B2B both parties know each other well and usually the transactions are of a high volume, repetitive nature, managed through private contracts. These contracts usually bind the businesses together, defining roles and responsibilities, and provide for ready made dispute resolution mechanisms. ODR is not yet a good dispute resolution method in B2B online disputes:

“ODR is not used to any meaningful degree in the B2B market segment since the parties have made other arrangements for the settlement of disputes between them and disputes among them are rare in any case.” [12].

With C2C e-commerce transactions the ground is more suitable for ODR than any other type of transaction. C2C transactions are growing and online auction sites like eBay [58] and uBid [136], are good examples of where C2C transactions can cause online disputes. In auctions, usually the dispute arises when either the seller or the buyer feels cheated and wants compensation or the item back. Most disputes are initiated by the buyer, where the item received did not satisfy expectations. If the seller did not satisfy the buyer or the two parties are unable to agree on some kind of compensation, direct negotiation and facilitated mediation ODR may be employed. (Using ODR does not affect the right of both parties to formal legal processes and remedies) [101].

6.6 ODR Conditions and Mechanisms

Since the use of ODR is mainly voluntary it must rely upon contextual fit, attractiveness, ease of use, and effectiveness to encourage implementation. As a means of redress it is

dependent upon the use of networked information technology and in its development has been dependent on what are deemed to be three 'essential building blocks' or conditions: trust, expertise, and convenience [80]. At the same time ODR can be offered via certain mechanisms or schemes that will also create added value and further trust in the whole process.

6.6.1 Building Blocks

Trust: Large scale online commerce is constrained by what has been described as a trust gap. Individuals and organizations are disinclined to trade without certain interactions and accountability. The extent of the gap is based on risk appraisal that will evaluate the likelihood of being able to reverse an unsatisfactory transaction as well as assessing the potential trading partners in question.

The law of contract has long been used to reduce risk by filling the trust gap with reliance on third party adjudication and enforcement. Trust is an interpretation or perception of the security this kind of mechanism implies, (i.e. the likelihood that object and compensation will be exchanged smoothly).

Although in offline situations, the existence of courts and ADR systems encourages individuals to have trust in what could be an unknown situation, in the online world this kind of 'trust gap' between buyers and sellers acts as a barrier. However ODR tries to remedy this situation by providing alternative ways to solve problems and alleviate doubts about trading partners.

Trust in the ODR process, for existing and future participants in terms of fairness and security, is essential, as is the likelihood of a reasonable resolution outcome should the need arise. In order to be seen to be fair the process should be neutral and open in its treatment and both sides should be given the opportunity to be heard. Trust is also paramount since security and the confidence that private financial or personal information will not be made public or inappropriately disclosed is a major concern for all concerned [101].

Expertise: The issue of expertise is closely related to that of trust. Prospective ODR users, and dispute resolution participants in general will be concerned with the quality of the system and process being offered. They will require evidence of expertise in form of third party ADR practice and fourth party ODR environment.

For any individual or business taking a claim to court, there will be an implied expectation about the quality of professional expertise involved in the process. The ADR ‘profession’ has been built up over many years and now represents a comprehensive knowledge base. This same kind of professional approach, in the form of technical expertise, is being built into ODR software systems. This is taking the form of structured communication and information management systems to facilitate use of direct negotiating systems and the settlement algorithms that are now used in ‘blind bidding’.

However in terms of building up its stock of experts and knowledge base ODR is still relatively new and in the process of development. Although it is taking much from the ADR example it still requires new skills and practices that are specific to the context of online transactions [101].

Convenience: Convenience is ODR’s major and most obvious advantage over formal litigation because of the ease with which dispute resolution can be delivered by IT and the obvious lack of physical costs. (Since online interaction can often occur between parties who are considerable distances apart, when disputes arise it is clearly more convenient to pursue resolution online than approaching a remote court to file a physical claim) [101].

6.6.2 Schemes

The most important schemes or mechanisms related to ODR service provision are described below:

(1) Universally Accessible Schemes

ODR services such as I-courthouse.com and Onlineresolution.com are available to any claimant trying to find redress regardless of the nature of the dispute. The main advantage of schemes such as these is the fact that they offer open access, although funding and

enforcement present two major disadvantages. For many small consumer claims the ODR service could prove too expensive since rather than being financed by membership fees, users themselves have to pay.

With regard to enforcement, if the business does not have ODR scheme membership it will prove much harder to implement decisions and settlements that have resulted from the whole process. The net effect is that independent schemes are much considerably less effective than those offering membership.

(2) Trustmark Schemes

The Trustmark scheme greatly enhances consumer confidence. As a result, various consumer and trade associations, government and also the private sector have established similar practices.

This approach enables the ODR provider to license the supplier with a logo or trustmark on its website. This provides an indication that the supplier is willing to partake in any dispute resolution scheme and that it will adhere to a prescribed Code of Conduct. This Code for example will require that any supplier should disclose company and contact details on their website and will guarantee to make delivery within an agreed time limit.

Therefore the trustmark should increase consumer confidence and give added value to the suppliers 'brand'. In return the supplier will pay a membership fee to be able to belong to the scheme and use the trustmark licence. The amount paid will also cover the cost of the actual dispute resolution process, in effect making the service free or at least relatively inexpensive to the consumer. If business members do not comply with the prerequisite standards of good practice they risk losing membership and their right to use the trustmark. Therefore the concept of the trustmark scheme is considered a very important factor in helping the development of consumer ODR services.

(3) Marketplace Schemes

The Internet marketplace itself often provides dispute resolution services, most commonly in the form of a site providing many suppliers of goods and services and in the form of either portals, auctions or shopping malls.

These types of marketplaces may also provide additional services such as dispute prevention mechanisms. Yahoo and E-bay, for example, provide the facility for a rating system on feedback about seller performance. This feedback can then be made available to future buyers as a way of helping make reliable selections about levels of trustworthiness and prevention of possible future disputes occurring. Some businesses will employ ODR providers usually to mediate in disputes, for example E-bay using SquareTrade.

Similar to trustmark schemes, suppliers who do not conform risk being excluded from the marketplace. This creates pressure on the supplier to comply and co-operate in any dispute resolution procedure [75].

6.7 ODR Requirements

Measures of effectiveness comprise only one of the criteria against which ODR is measured. Equally important is that the procedure should be fair [75]. Significant factors such as independence, impartiality and transparency are outlined below.

6.7.1 Independence and Impartiality:

In any ODR case, both ODR provider and the arbitrator/mediator must be considered to be independent, impartial and free from any personal interest in the eventual outcome.

Since it is unavoidable that either the merchant or the customer will provide the funding for the process this should be compensated for by assurances that independent third parties will supervise the overall scheme and represent consumer interests in an impartial manner. However this is an ideal situation: in reality these requirements are rarely evident in existing schemes.

Individual arbitrators or mediators are also required to observe codes of professional ethics requiring them to disclose personal interests in order to avoid conflicts of interest. Evidence of this type of compliance should be made available to the user. Furthermore,

allocation of arbitrators should be random and no one party should be allowed to make the choice [75].

6.7.2 Publicity and Transparency

Secrecy and confidentiality are paramount in out-of-court situations and the same should be expected in ODR proceedings. Nevertheless in order to further develop openness in the ODR process wider public policy concerns may prove to be an overriding issue. For example, where instances of widespread business malpractice in the mass consumer e-commerce market have occurred, the public has a right to be made aware of these situations. If ODR is to become the dominant form of e-commerce dispute resolution, arbitration decisions that have been reached should be used to form a substantial body of new law, helping to eliminate uncertainty in terms of the rights and obligations of e-commerce parties. Indeed, e-commerce 'law' is not likely to develop any further and become transparent if these types of decisions are not public. This complex issue of transparency will become even more crucial if ODR develops as the predominant form of dispute resolution for e-commerce in the future.

The ICANN dispute procedure established to resolve the registration of domain names such as '.com' provides a good example. This 'Uniform Domain Name Dispute Resolution Procedure' (or UDRP) is published on the ICANN website [100] and as a result a body of case law in this area is developing.

If decisions are not published, a 'one-time only' user is not likely to be aware of what has previously been established and become acceptable as law. On the other hand, regular users (usually suppliers), are likely to have an unfair advantage by knowing what has been established in the past. In addition, unless there is sufficient transparency through the publication of results it will be impossible to check the quality and impartiality of dispute resolution and therefore the integrity of the whole system [69].

Online published statistics are only likely to amount to the numbers and types of disputes that have been resolved at present due to the informal nature of the process. However, ideally, these decisions should be published but unfortunately there is no legal obligation for ODR providers to do so at this moment in time [49]. To be truly transparent, ODR

schemes should also be clear about rules, standards and aspects of the law that have been employed as a basis for reaching some kind of settlement or decision [60].

6.7.3 Language Barriers

Most ODR providers do not give sufficient attention to the problem of cultural and linguistic differences. Currently ODR services are offered in English and only very few offer a bilingual or multilingual service[49].

6.7.4 The Right to a Fair Hearing, and Ability to Respond

Entitlement to a fair hearing implies that each party be given an opportunity to state their case and hear and respond to the other party's submissions. Since ODR schemes usually rely on written (web-based or email) submissions by the parties they should be allowed a fair amount of time in which to respond.

6.8 Dispute Processes

Most dispute case would follow the flow of Figure 6-1:

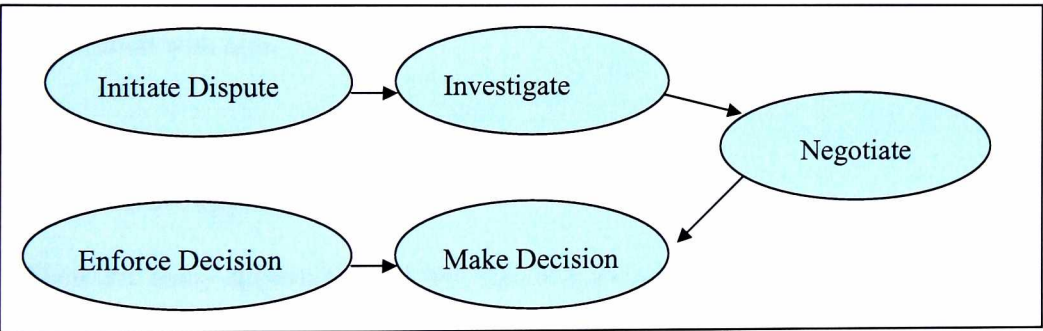


Figure 6-1: Dispute Processes

Dispute Initiation: the affected party, whether individual or organization, approaches a dispute resolution authority, files a claim for examination of the dispute (either online or with a mixture of online and offline components) if he feels there is some entitlement to redress.

Dispute Investigation: the dispute resolution provider or any other party handling the resolution will solicit participation from the non-complaining disputant through email, phone, fax, or snail mail. Once there is agreement on both sides for participation the provider will begin to examine the claim by collecting evidence and information about the case.

Dispute Negotiation: having collected the necessary information the dispute resolution provider will negotiate possible resolutions with both parties.

Making the decision: if the dispute resolution provider has the authority to require both parties to follow the suggested course of action then a decision will be made regardless of whether both sides are happy with the outcome. However, if no such power exists then the agreement of both parties is necessary before a decision can be reached.

Decision Enforcement: the most difficult, but at the same time the most crucial, stage in the whole process since all of the previous stages will have been pointless if enforcement cannot be made. In most cases this stage will be conducted by a party other than the dispute resolution provider.

If enforcement cannot be instigated, at the very least a negative 'mark' should be assigned to the refusing party of making any future participants wary of entering into any transaction with him.

6.9 ODR Approaches

There are many approaches to ODR, the most basic of which are negotiation, mediation and arbitration; the remainder discussed in this section, i.e. evaluation, decision support systems and virtual courts, are some of the most widely used variations of these three approaches.

More specific distinctions within the ADR concept, such as "arbitration", "mediation" and "conciliation/negotiation", are often used interchangeably and without much

precision. Such distinctions may, however, be of relevance with regard to the role of the dispute resolver(s) in the process and the enforceability of the results [56].

6.9.1 Negotiation

Direct and automated are the two types of negotiation available in dispute resolutions. In the case of direct, the ODR provider links two parties (or more) using conventional media such as snail mail, phone or email to enable communication. Automated negotiation, on the other hand, is a computerized process designed in the main to settle monetary disputes.

SquareTrade [126] has established a direct negotiation ODR system for eBay. It now handles 80% of its auction related disputes and has overseen the successful resolution of over 66% of cases [81]: in only one day it has been known to have handled over 1000 complaints. Nevertheless, whilst this form of direct negotiation requires no human facilitation by SquareTrade, for other online disputes simply enhancing communication is not enough to be able to settle conflicts [101].

As an example of automated negotiation, systems based on blind bidding such as those offered by CyberSettle [53] and Clicknsettle [46], will apply ‘Split The Difference’ algorithms, where secret bids must come within a pre-agreed range and participants never get to know the exact demands or offers being made. The only knowledge they are given is based on their bid. As a result they may be required to make a further submission or be told that the resolution has been successful or unsuccessful [101].

Such systems are suitable for monetary claims where liability is not disputed and only the amount of the compensation is at stake, as in the case of e.g., insurance claims. [76].

6.9.2 Mediation

The mediation process, whether described as ‘assisted negotiation’, ‘facilitation’ or ‘conciliation’, involves the use of a third party in order to facilitate resolution dialogue without having to resort to intervention between the two parties that reaching a fair compromise is their concern.

However the use of the term mediation means that the neutral third party has to be proactive in looking for solutions and as a result will talk separately to both parties. Only when both parties agree upon a final mediation proposal can it be turned into a contract and therefore be enforceable. If no compromise is reached, both parties are entitled to resort to another dispute resolution method or take their case to court [56].

Mediation will take the form of a series of communication exchanges at the ODR mediator's web site. The mediator in question will employ techniques similar to those of their offline counterparts but without much of the informal information exchange evident when there is close physical proximity, e.g. body language, tone of voice, eye contact. Since many dispute cases follow a similar pattern, online mediators such as those in SquareTrade will be able to develop a reliable knowledge base and set of practices in order to manage situations such as auction related disputes effectively.

Mediation appears to be the main ODR method for small value disputes and in this context has many advantages. The process is flexible, parties have a high degree of control enabling them to feel at ease with the whole online procedure and encourage its use. The mediator will basically use his skill to help the parties communicate and reach their own solution.

Redress is not limited to monetary awards: parties can explore solutions based on future interests and not just past rights. For example, an adequate response to a consumer complaint could be a substantial discount from a future purchase or similar, ensuring that both parties are satisfied with the outcome.

If successful, business relationships are also likely to remain intact since the types of dispute arising from small value e-commerce transactions are usually more a matter of customer service than that of conflicting rights.

When successful, mediation is also much faster and cheaper than arbitration and going to court. On the other hand however, the disadvantage of the consensual nature of mediation is that it is not always successful. The whole process could prove to be a waste of time and money if it fails to reach a solution. The likelihood of success is further threatened by its lack of authority since it is a non-binding procedure [102]. Also, the involvement

of the human element as mediator within the online system may also prove too expensive for small value claims since fees can normally range anywhere between US \$20-200 [76].

For the majority of cases the success of mediation is purely dependent on the merchant's desire to maintain good customer relations and so for that reason it is often argued that the success of the whole process rests merely on the relationship between the two parties. Where there is continuity in the business relationship more effort will be put into resolving any dispute than those where transactions are only one-off occurrences.

6.9.3 Arbitration

Usually arbitration is a process where a neutral third party – an arbitrator – invites the parties to submit the facts and their arguments (oral and/or written procedure) and finally makes a decision based on the appropriate legal rules. The arbitrator's decision is intended to be binding and thus usually may not fit easily to the non-jurisdictional world of trans-border B2C transactions

Securing the agreement of the parties, usually the business, to binding arbitration after the dispute has arisen is a difficult problem and the only time it is secured is when the business subscribes to an arbitrator and publishes this in his website.

The Internet is very suitable medium to documents-only arbitration, but online consumer arbitration, as opposed to online mediation and other methods of ODR is not very common.

The fees for arbitration must be proportionate to the value of the claim. But arbitration requires the involvement of a qualified and experienced human arbitrator also e-commerce disputes are mostly of small value, so this may be difficult or impossible to achieve. For this reason, and many others, arbitration is not the first choice for small and medium value e-commerce disputes. However, under some schemes, online arbitration is used as the last resort layer of a scaled approach to ODR. In such schemes the parties start with negotiation and if this fails they move on to mediation and only if this fails will they resort to arbitration [76].

The main advantage with arbitration is that both parties are able to choose the arbitrator and also which legal rules apply. Any final decision could also be enforced internationally. In order for the process to work effectively, points concerning the governing law, rules of arbitration (usually through the choice of a provider), the place of arbitration (even if the process is to take place on line) and the number of arbitrators (the lower the cheaper) need to be mutually agreed [102].

6.9.4 Evaluation

Evaluation is a special form of arbitration. Online evaluation involves a neutral third party making a decision on the basis of written submissions and documentary evidence provided by both sides. However the decision will only take the form of a non-binding recommendation but this may make it easier to secure the participation of the other side after a dispute has arisen [76].

6.9.5 Decision Support Systems

Decision support systems could also be described as a multi-variable negotiation systems. They provide a special form of negotiation where third party facilitators take active roles in assisting participants to identify, quantify, and adjust preferences in robust fourth party environments. For example SmartSettle according to them, will aggressively leverage computational information technology as much as information management and communication in order to reach a satisfactory resolution. The system users break disputes down into basic operative variables that are given discrete value ranges, and represent a mix of interests that can be adjusted during negotiations. Users will adjust variables as they wish, after that they view the resulting satisfaction index. If the satisfaction index is not good enough they will propose a new combination [133].

6.9.6 Virtual Courts

As part of the ODR process, virtual courts, such as I-courthouse.com, emulate elements of real courts and their processes. Cases can be originated either online or offline and both parties to the dispute will be provided with the opportunity to present a narrative claim with supporting evidence in this fourth party environment. All communications in

the virtual courts take place via the Web, and usually maintain basic document management. A jury of peers shares the same environment and acts as third parties who may query disputants individually and then render non-binding decisions. Unless a contractual agreement results, findings are usually not binding [76, 101].

6.10 Critique Of Current ODR Systems

From the above arguments it can be clearly observed that none of the current ODR methods are completely automated, negotiation being the process that comes nearest. However even negotiation lacks reliability, and only works for a small domain of disputes where the major concern is usually the amount of money being contested. Mediation is very costly if unsuccessful and the need for human involvement as part of the process makes the cost even higher. Arbitration, on the other hand is not automated due to the complexity involved in covering all cases and the difficulty in verifying documents automatically online [21]. Therefore, in all of the current ODR methods, even though the cost of redress may be lower than the normal cost of going to court, it is still high compared to the value of the products which may sometimes be as little as £5 or less.

An examination of three of the best known websites involved in online dispute resolution demonstrates that they are not particularly suitable for their purpose, rather they survive by taking advantage of consumer ignorance where there is a lack of knowledge about rights or on the other hand, exploiting the willingness of merchants to make small losses on transactions in order to maintain levels of customer satisfaction.

Taking the example of SquareTrade [126], the official dispute resolution company that handles eBay disputes, it offers two services: negotiation, which is free and mediation, which will cost at least \$20 as Figure 6-2 shows. Online direct negotiation systems such as this one are web and email based, with claims and responses filed via a web interface. Exchanges are subsequently facilitated through email message scheduling database and routing software. As a result this form of direct negotiation requires no human facilitation by SquareTrade.

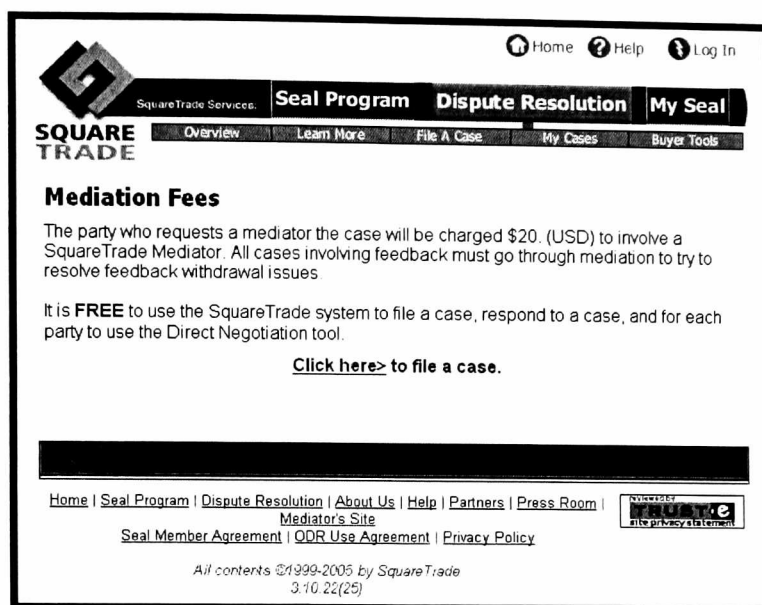


Figure 6-2: SquareTrade Mediation Fees(1)

Source: [126]


Negotiation offered by squareTrade merely involves completing an appropriate online form that asks for a description of the problem. This is then forwarded to the other party in the dispute. The company will then inform the dispute Initiator that contact will be made again with the opposing party after a certain period of time if no response has been forthcoming.

After three months if there is no evidence of any kind of response from the opponent the case will be closed. Although this might result in a lack of profit for SquareTrade, the reality is that it could result in even greater loss for the dispute Initiator since most of the time after three months credit cards issuers will not accept any dispute regarding the transaction [21].

Therefore a more appropriate way to resolve the situation might be for the dispute Initiator to write to the other party directly and if no reply is received, to contact the credit card issuer and dispute the charges immediately.

Mediation offered by SquareTrade has a further major problem apart from the cost/profit issue and this is that any result is not binding on the parties concerned. SquareTrade has

a minimum charge of \$20 for some of the better known marketplaces such as eBay. However this could be deemed high since most of the e-commerce transactions it will be dealing with will be around this kind of value and at the same time resolution is still not guaranteed. For other merchants who do not subscribe to SquareTrade the minimum charge is \$40 as shown in Figure 6-3.



Home

Help

Log In

SquareTrade Services

Seal Program

Dispute Resolution

My Seal

SQUARE TRADE

Overview

Learn More

File A Case

My Cases

Buyer Tools

Mediation Fees

The cost to involve a mediator in your case is as follows:

Transaction	Mediation Fee (paid by party requesting the mediator)
Up to \$1000.	\$40.
Above \$1000.	\$40. plus 5.00% up to a maximum of \$2500.


It is FREE to use the SquareTrade system to file a case, respond to a case, and for each party to use the Direct Negotiation tool

[Click here> to file a case.](#)

Figure 6-3: SquareTrade Mediation Fees (2)

Source: [126]

Only one company, SONY actually offers to pay the mediation charge instead of the disputant as shown in Figure 6-4. However not all merchants are as big as SONY and therefore able to offer such a service.



Home

Help

Log In

SquareTrade Services

Seal Program

Dispute Resolution

My Seal

SQUARE TRADE

Overview

Learn More

File A Case

My Cases

Buyer Tools

Mediation Fees

It is **FREE** for consumers to file a dispute and engage in online mediation with Sony Electronics Inc. (Sony) using SquareTrade. Sony will be charged separately.

[Click here> to file a case.](#)

Home | Seal Program | Dispute Resolution | About Us | Help | Partners | Press Room | Mediator's Site

Seal Member Agreement | ODR Use Agreement | Privacy Policy

All contents ©1999-2005 by SquareTrade

3/10/22(25)

Figure 6-4: SquareTrade Mediation Fees (3)

Source: [126]

SmartSettle [125] works by making a preference analysis summarizing how parties in each dispute reach some satisfactory outcome. On the basis of this information SmartSettle can generate future proposed solutions that will maximize satisfaction for all parties. The price of the lowest possible tool is \$100. It is clear that such system is expensive and for that reason it is not open to the public.

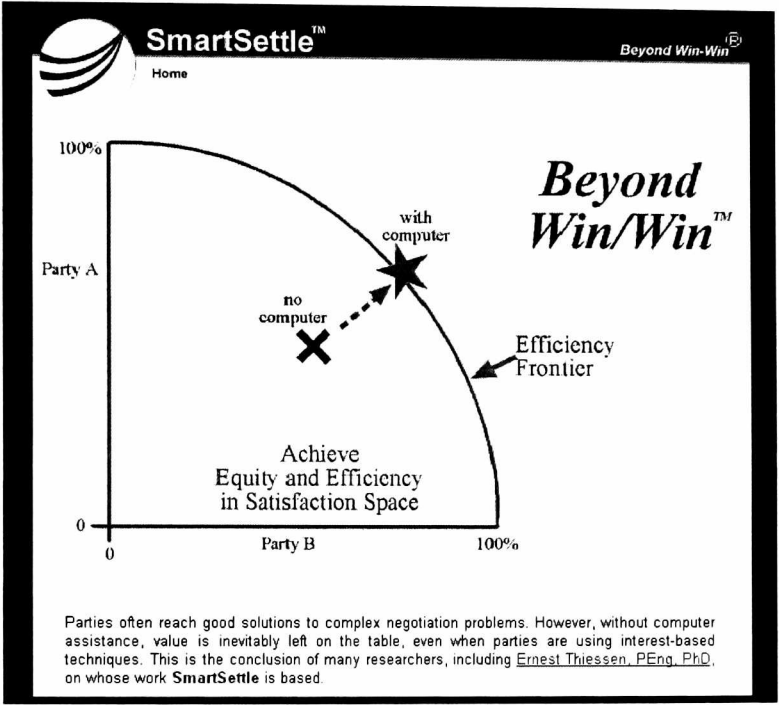


Figure 6-5: SmartSettle Dispute Resolution Method
Source: [125]

Cybersettle [53] will try to use some algorithms to find a solution that will satisfy both parties and claim that as a result they can reach resolution that will exceed the expectations of both parties. However, the question ‘Can non-represented claimants use Cybersettle?’ was answered in their FAQ page with a negative reply ‘No, Only attorneys and claims professionals are able to participate in the Cybersettle process’. Moreover, the example given in their website, see Figure 6-6, is probably not very appropriate to demonstrate this point since it assumes that both parties will be willing to give something every time they are asked.



Figure 6-6: Cybersettle Dispute Resolution Method

Source: [53]

6.11 Conclusion

Due to the increasing importance of dispute resolution and the continued demand for low value e-commerce items, an automated online dispute resolution must be developed that is able to receive complaints with supporting evidence and come up with a fair resolution automatically (and promptly).

If such a system could be fully automated then the cost of dispute resolution would be minimized and would be deemed appropriate for all low value disputes. Initially such a system should be able to resolve even just a small domain of disputes fairly in order to become established and gain credibility. In the future, as e-commerce and its customers mature, increasing numbers of cases can be resolved using the same system with little or no improvements being needed.

The following chapters will propose and appraise a new system intended to answer these problems. Since the proposed new system will not be able to function fully in the current e-commerce infrastructure, next chapter will propose an ideal or optimum infrastructure to support the new system.

CHAPTER SEVEN

E-commerce Transaction Protocol

CHAPTER SEVEN

E-commerce Transaction Protocol

7.1 Introduction

One of the major problems identified in current dispute resolution methods described so far is the human element. This can result in major excessive expense, even where this type of involvement is kept to a minimum. The problem is even more evident when dealing with soft products such as E-books, audio tracks, software etc. because these are goods which are intangible, require no physical shipping and are usually of very low value in relation to the potential cost of the dispute resolution.

Research in this thesis has proven that the only really effective way to lower the cost of resolution is to automate the entire process. Chapter 8 will describe this process in detail, meanwhile this chapter will describe the E-commerce Transaction Protocol (ETP) needed to facilitate this new development. The ETP is needed due to the fact that the proposed new system of automating the resolution process would not be able to function correctly with the current e-commerce infrastructure. This need is caused by the lost of trust in the Internet due to cross border transactions, the financial benefits that have been derived from these fraudulent transactions and the introduction of new products and services such as soft-products.

In order to solve this problem the thesis will offer a complete solution. The solution will comprise two parts (i) an E-commerce Transaction Protocol (ETP) that is practical and expandable to accommodate any new improvements in the future, and (ii) an Automated Online Dispute Resolution (AODR) system which should automatically resolve any dispute happening within the proposed e-commerce model.

This chapter will discuss the e-commerce transaction protocol in general, its components and how it works. The terminology used is already well-known, the intention is not to create a new technology, rather its intention is to build upon existing knowledge by modifying and suggesting improvements to better satisfy technical needs. This chapter

will also demonstrate the proposed concept of assigning a quality certificate to every soft-product.

7.2 E-commerce Transactions

E-commerce is now the most important and the fastest growing kind of transaction in all parts of commercial activity. An e-commerce transaction is a means to perform particular commercial activity using the global digital e-commerce infrastructure. Because of this importance a huge number of people are investing in it. The main advantages of the e-commerce are its global nature, its simplicity and low cost compared to normal face to face business.

During the last ten years e-commerce has developed swiftly, and many improvements have been made to try and reach the optimum E-commerce transaction. An optimum E-commerce transaction would be one in which all of the transaction processes were done automatically online with the minimal time, effort and cost.

As a general principle, each transaction will normally involve several processes, as illustrated by Figure 7-1. Each of these processes and their current state-of-art in terms of automation is listed below:

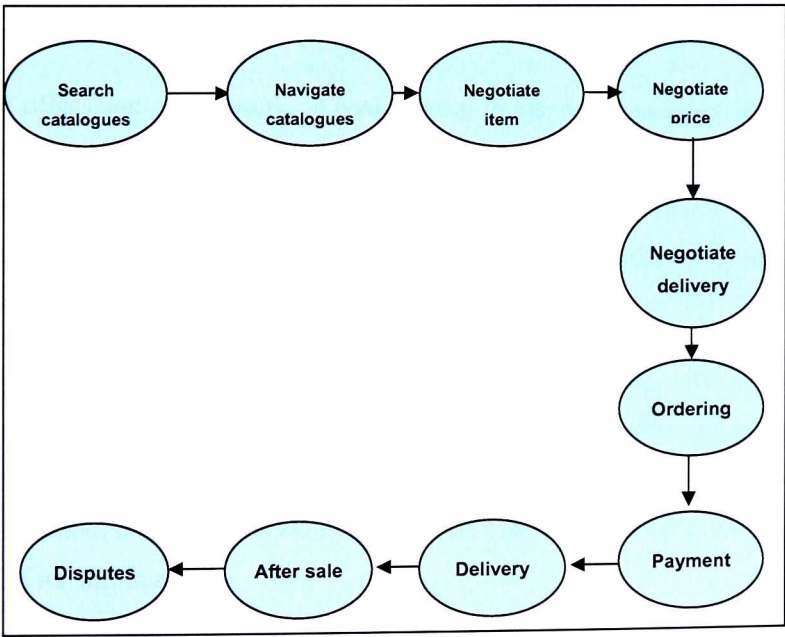


Figure 7-1: E-commerce Processes

Searching for catalogues: with the huge improvement in search engines and search methods (e.g. yahoo.com and Google.com), this aspect of the transaction is now considered one of the easiest to undertake using the Internet. Therefore searching for catalogues has probably already reached the optimum level and will be easy to incorporate into any new developments.

Navigating the catalogues: each e-commerce site has developed its own route to enable customers to navigate its catalogues. Much research has been conducted in order to maximize this process and better align the routes being offered to customer thought processes and patterns of logic [45].

This issue is also reaching the optimum level since it relies purely on the effectiveness of the technology and as a consequence the need for human interaction within the process is eliminated. However some sites are still not as advanced as others and in consequence at the moment there is still be a need to employ people to explain to customers how and where they can find the products they are looking for.

Negotiation: item, price, delivery: all these negotiations can be done completely online and with no human interaction since options will be offered at each stage in the decision making process.

Merchant offers and promotions are also offered in this way to all customers without their ever having to contact the site. If the merchants want to offer specific services to specific customers they will offer a series of preferred membership classes where prices could change according to a set of pre-determined criteria. Alternatively other promotional codes might be programmed into the site in question.

Ordering: consumers in the past have been used to face to face interaction in this stage of the transaction, technological development has now made this a very simple and automated procedure. As a result many companies have now developed a one stop ordering method, therefore this stage can also be considered to have reached the optimum in terms of its automation.

Payment: this is the most complicated stage in the e-commerce transaction process for many reasons. First, the huge number of payment methods available makes the process of total automation difficult. Second, the fear of fraud when using traditional payment methods like credit cards and wire transfer make people reluctant to use these facilities online. Even though such complications exist, businesses, especially those who accept credit cards or e-payment methods, manage to make the payment process fully automated and therefore are able to eliminate the need for human involvement. This stage of the process could therefore be described as still being in the process of reaching the optimum stage.

Delivery: this stage in the process is highly dependent on the nature of the item that has been purchased since some items, e.g. laptops, cannot be delivered electronically. Due to their physical nature, total automation at this stage will therefore be impossible. However, in the case of soft products [16] businesses are able to deliver these items automatically online and without any human involvement. Systems have now been developed to deliver these items automatically once payment has been approved and are therefore fast approaching optimum level [42].

After sales service: this includes the warranty, updates and support. With the help of new technologies some businesses manage to automate all of these issues, for example automatic update features in some software. Some sites also offer automated compliant systems and maintenance like Sony.com. However research to date has not shown that this stage is fully automated yet and further research is probably necessary in this area.

Dispute: this stage could also be considered as an after-sales service but since many businesses choose not to offer this aspect or participate in it, it has been shown as a separate stage in Figure 7-1 and as a result it leaves the customer with no opportunity for redress. This particular stage is the least served in terms of automation, as chapter 6 has shown.

7.3 Protocol Requirements and Components

The e-commerce transaction protocol is generic and therefore should fit with any type of product and payment method. Therefore money in any form can merely be treated as another type of product that one party wants in exchange for the other party's product that is being offered.

7.3.1 Protocol Requirements

Before deciding on the infrastructure needed to support the protocol, it is clear that in any transaction there are at least two parties involved: seller and buyer or merchant and customer.

Certain components are essential to support the infrastructure. Analysis of the research that was undertaken to find these components involved an examination of every dispute possibility. These are now summarized below and since money and goods have been treated in the same way only one case of every possibility has been considered.

Item1 delivered but Item2 not delivered ($Dx \ \& \ \neg Dy$): The above case requires proof of delivery

Item1 not delivered on time ($\neg Ty$): The above case requires the proof of delivery to be time stamped and also a proof on the agreed delivery time

Item1 can not be delivered ($\neg Ax$): The above case is more complicated than the previous two and it requires proof of attempt to deliver or proof of failed delivery.

Party1 claims never agreeing in an exchange ($\neg Px$) : This case requires proof of identity showing that the other party agrees to participate in this transaction.

Item1 quantity is not correct ($\neg Cy$) : This case requires proof of quantity, also a proof on the agreed quantity.

Item1 received not as agreed ($\neg Iy$): This case requires proof of delivery, of what was being delivered and on the agreed item for delivery.

Quality of item1 received not as promised ($\neg Qy$): Quality of items has to be known and also delivery proof should include quality of the item delivered and proof of the agreed quality

Item1 received not as expected ($\neg Sx$): Level of satisfaction should be agreed on before the transaction. This can be anything on a scale of 0-1 where 0 = no satisfaction guaranteed at all and 1 means satisfaction is fully guaranteed where the guarantor will pay all expenses if satisfaction is not achieved. So a proof on the agreed satisfaction level should be provided.

Item1 consumed twice ($\neg My$): This case requires proof of the number of times the item was consumed.

From the above observations the requirements can be summarised as follows:

- *Proof of delivery or attempted delivery showing time, item, quantity, delivery result and result justification;*
- *Proof of agreed terms showing identity, item, quality, quantity, delivery period, delivery address and satisfaction level. This can also be described as Contract Terms;*
- *Proof of quality: proving the quality of the item delivered.*

7.3.2 Protocol Components

From the above findings it can be concluded that the E-commerce transaction infrastructure consists of two conventional players (the traditional customer and merchant) and three trusted third party (TTP) servers. The three servers are as follows:

Quality server: a global trusted third party who will be issuing the quality certificate of all soft products before the transaction. Each of the two parties should have the item quality certified by a Quality server, and advertise that the quality of the item has been certified by this server.

Contract server: this server is the one who will certify that the contract has been made between the two parties. In consequence both parties should trust this party. This third party server situation is simple in the sense that it receives two inputs having the same transaction ID from the customer and the merchant and then ensures that two inputs are identical. As a result it will then be able to confirm both parties that their agreement is a match and they can go ahead and start the exchange. This server should be able to provide a certificate showing the inputs that correspond to the transaction ID.

Delivery server: each party should be able to choose a Delivery server that is trusted. This server will receive all the items sent to the party and makes sure they are delivered to the party in question in a correct time and form. Therefore total trust is placed in the Delivery server and there is absolute confidence that the items ordered will be delivered if the Delivery server receives it.

If the other party is not confident with the selected Delivery server, they can request a change. This server is the place where all the items for specific parties will go first. The Delivery server should be able to confirm any delivery by signing the information received and append to it some delivery variables like time of delivery and sending it back to the sender.

Having briefly explained the roles of each of the three TTPs, a complete description of each will now be given, showing its internal processes and how it works.

7.4 Contract Server

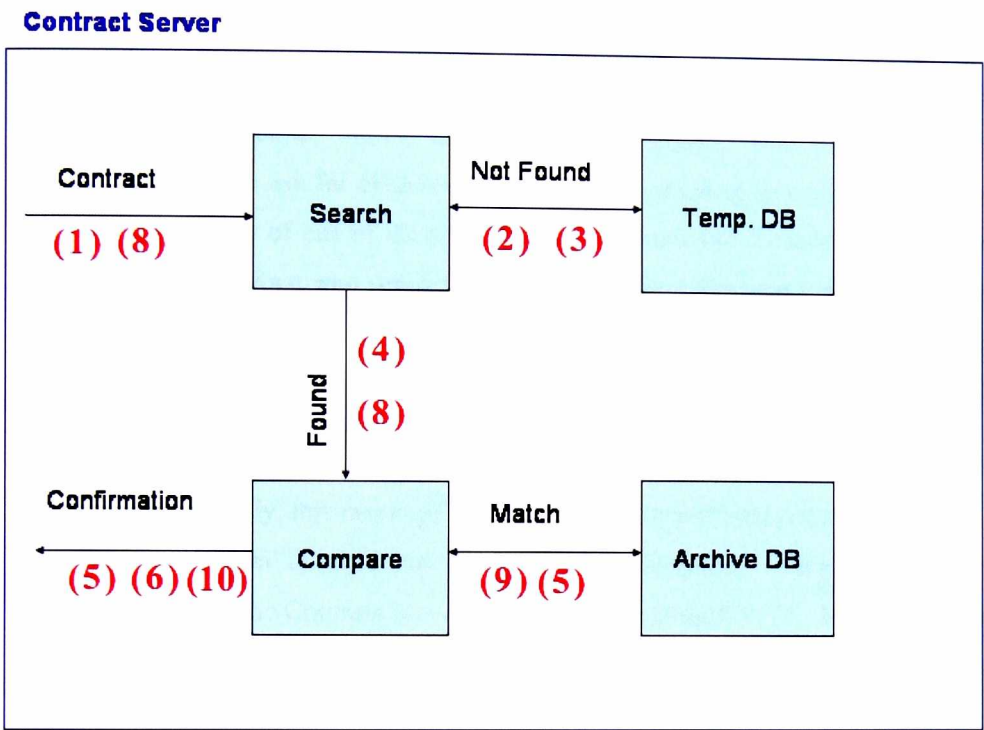


Figure 7-2: Contract Server Architecture

(The numbers referred to in the diagram are described in the Services section below)

Messages

- a) The Contract message is to be sent by both parties. It contains the Sender ID (X), Transaction ID (T), and the Contract (C_{XY}-C_{YX}), the last two are encrypted by the sender's private key: **Contract(X, [T, C_{XY}-C_{YX}]_X)**
- b) The Confirmation message: this message is sent to both parties and it contains the Contract server ID (CS), Transaction ID (T), Status of the contract (Stat) and the agreed terms (C_{XY}-C_{YX}). Everything except the Contract server ID is encrypted by the Contract server's private key. There are two types of confirmation [Match and Mis-Match]. In the first case the two contracts will match and the status will be designated [M] and the agreed terms will be sent. In the second case where it is a

Mis-Match the status will be designated [MM] and the mis-matched terms will be sent: **Confirm(CS, [T, Stat, Cxy-Cyx]_{CS})**

- c) Evidence Request: this message is sent by one of the two parties asking for a confirmation of the contract to submit to the dispute resolver. The Contract server could be "Locked" which means that only people who participated in the transaction can ask for evidence. This involves sending an encrypted message by the private key of one of the two parties. Alternatively it could be "Open" which means that anyone who sends the evidence request message will get the reply. As a privacy issue it is recommended that the default be Locked. The message contains the requester ID (X) and the Transaction ID (T), the latter will be encrypted by the requester's private key: **EviReq(X, [T]_X)**
- d) Evidence supply, this message will reply with the archived contract matching with the Transaction ID received in the EviReq Message. This message will be encrypted by the Contract server private key: **EviSup(CS, [T, Stat, Cxy-Cyx]_{CS})**

Services

This server provides two services; one confirms the matching of contracts as follows:

- (1) One party sends a contract to the server **Contract(X, [T, Cxy-Cyx]_X)**.
- (2) The server searches the temporary database of the contracts that have not yet been confirmed for a transaction that has the same ID;
- (3) If nothing has been found in the temporary database, then this contract is indexed and stored in the temporary database;
- (4) If a match is found, the server will compare the stored contract with the new one;
- (5) If contracts match, confirmation will be sent to both parties **Confirm(CS, [T, M, Cxy-Cyx]_{CS})** and one copy will be saved in the archive database;

- (6) If the two contracts don't match, a negative confirmation will be sent to both parties **Confirm**(CS, [T, MM, Cxy-Cyx]_{CS}) telling them that a mismatch happened in their contracts and the mismatched terms will be included;
- (7) The two parties are free to revise their contract and send them again with a new transaction ID or abort the transaction.

The second service supplies evidence of an agreement on a contract as follows:

- (8) One party sends a request **EviReq** for evidence by encrypting the transaction ID with the necessary private key.
- (9) The server checks the archived database and if the contract is found and the requester is recognized as being one of the parties participating in the contract, if the server is locked, an **EviSup** message of the agreed contract will be sent to the requester encrypted by the Contract server private key.
- (10) If no match is found in the archive an **EviSup** message will be sent back to the requester with the status 'Not found'.

Points to be considered

- There should be a way to generate ID for the transaction or contract so that no two transactions can have the same ID.
- Every Contract server specifies a time limit, e.g. 48 hours, for the temporary database so if no correspond order arrives within this limit it will remove it in order to save space on the server.
- Every Contract server specifies a time limit for the archived database e.g. 4 months or the maximum dispute period, so it will remove it to save space on the server.
- The time limits could be incorporated in the contract itself to give the two parties the opportunity to choose the suitable limit.

7.5 Delivery Server

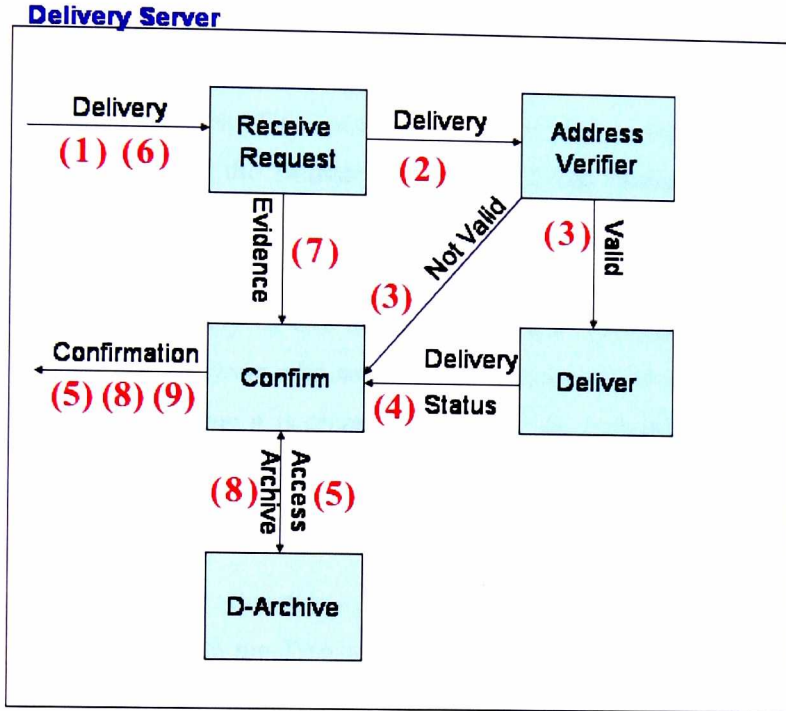


Figure 7-3: Delivery Server Architecture

(The numbers referred to in the diagram are described in the Services section below)

Messages:

- The Delivery message is to be sent by both parties. It contains Transaction ID (T), Item (I), Delivery Address (A) and the count of Items (C): **Delivery(T, I, A, C)**
- The confirmation message: this message is sent by the Delivery server to the party who is delivering the item to confirm receipt of the item. It contains the Delivery server ID (DS), Transaction ID (T), item (I), address it was delivered to (A), the count of Items(C), time of delivery (TD), and the Status of the delivery (Stat). Everything except the Delivery server ID is encrypted by the Delivery server private key. There are three types of status [Delivered, Invalid address, Not-delivered]. Where the item is delivered correctly the status will be [Delivered], if

the address supplied is not correct the status will be [Invalid address], and if the server can not deliver the item for any reason other than the invalidity of the supplied address, which means that this is not the mistake of the deliverer, the status will be [Not delivered]: **Confirm(DS, [T, I, A, C, TD, Stat]_{DS})**

- c) Evidence Request: This message is sent by one of the two parties asking for a confirmation of the Delivery to submit to the dispute resolver. The Delivery server could be "Locked" which means only people who participated in the transaction can ask for evidence and that requires sending the message encrypted by the private key of one of the two parties. Alternatively it could be "Open" which means anyone who sends the evidence request message will get the reply. As a privacy issue it is recommended that the default be Locked. The message contains the requester ID (X) and the Transaction ID (T), the latter will be encrypted by the requester's private key: **EviReq(X, [T]_X)**
- d) Evidence Supply: this message will reply to the EviReq with the archived delivery that matches with the Transaction ID received. If no matching is found the reply will be the Transaction number and the remaining fields are zeros. This message will be encrypted by the Delivery server's private key: **EviSup(DS,[T,I,C,A,TD, Stat]_{DS})**

Services:

This server provides two services [20], the first of which is delivering an item to one of its subscribers. This first process is described below:

- (1) One party sends a Delivery request **Delivery(T, I, A, C)** to the server;
- (2) The Receive Request process takes the request and time-stamps it and then sends it to the Address Verifier process;
- (3) The Address Verifier checks the validity of the supplied address and if it is valid it will send every thing to the Deliver process. If the address is not valid it will send an invalid status [Invalid address] reply to the Confirm process.

- (4) The Deliver process will try to deliver the item to the address supplied. If the delivery was successful it will send a positive delivery status [Delivered] to the Confirm process. If for any reason- for example mail box is full- it will forward a negative status [Not-delivered] to the Confirm process.
- (5) Confirm process will perform an archiving step before replying to the deliverer with the result of the attempted delivery **Confirm(DS, [T, I, C, A, TD, Stat]_{DS})**. This reply contains the time of delivery and status signed by the Delivery server's private key.

The second service supplies evidence on Delivery as follows:

- (6) One party sends a request for evidence by encrypting the transaction number with a private key **EviReq(X, [T]_X)**.
- (7) The Receive Request process forwards this request directly to the Confirm process.
- (8) Confirm process will check the archived database and if the delivery is found and the requester was one of the parties participating in the delivery, a copy of the delivery will be sent to the requester encrypted by the Delivery server's private key **EviSup(DS, [T, I, C, A, TD, Delivered]_{DS})**.
- (9) If no match is found in the archive an **EviSup** message will be sent back to the requester with the transaction ID and all the other fields as zeros meaning that this delivery was never attempted. **EviSup(DS, [T, 0, 0, 0, 0, 0]_{DS})**

Points to be considered

- There should be a way to generate IDs for the transaction or delivery so that no two transactions can have the same ID;
- Every Delivery server must specify a time limit, e.g. 4 months, for archive database so delivery evidences will be removed to save space on the server.

7.6 Quality Server

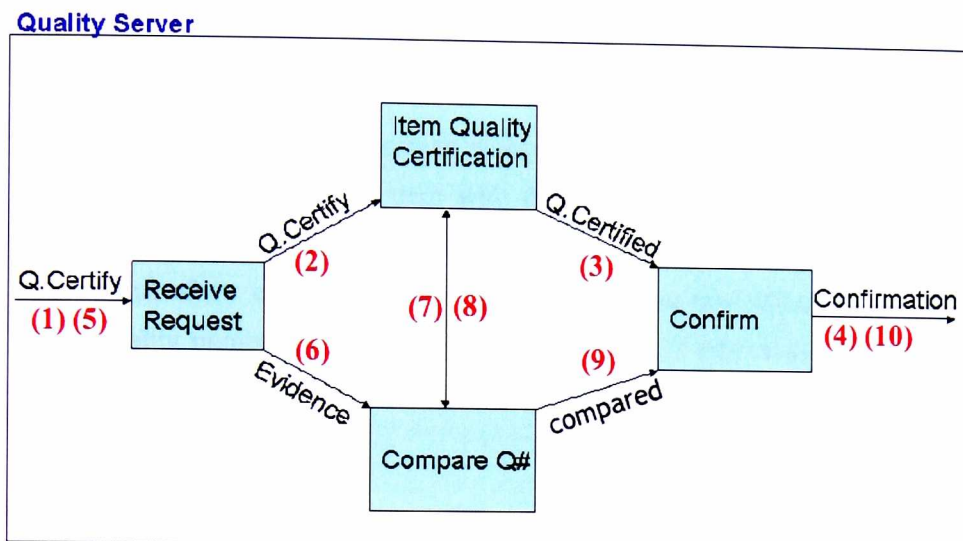


Figure 7-4: Quality Server Architecture

(The numbers referred to in the diagram are described in the Services section below)

Messages

The Quality server has four messages

- The Quality Certify message to be sent by both parties, containing the Sender ID (X) and the item to be qualified (I): **QCertify(X, I)**
- The Quality Certified message: a confirmation message sent to the party requesting it. It will contain the Quality server ID (QS), the Item (I) and the Quality number (Q#). Everything except the Quality server ID is encrypted by the Quality server's private key. There are two types of confirmation, 'certified and 'unable to certify'. In situations where an item is certified correctly the Quality number will be assigned a unique positive integer number [INT] from this server. In cases where, for any reason, the item could not be certified the Quality number will be [-1]: **QCertified(QS, [I, Q#]_{QS})**

- c) **Verify Quality**: in this message one of the two parties or even the resolving party sends the request asking for confirmation if the given item has the supplied Quality number. The message contains the sender ID (X), the item (I), and the Quality number (Q#): **VerQty(X, I, Q#)**
- d) **Quality verified**: this message will reply with the result of comparing the actual Quality number of the item with the Quality number supplied in the VerQty message. It contains the Quality server ID, the item, the Quality number and the status of the comparison. The status would have two values: [T] if the supplied Quality number matches the actual one or [F] if they mismatch. This message will be encrypted by the Quality server's private key: **QtyVer(CS, [I, Q#, Stat]_{QS})**

Services:

This server provides two services, the first of which is Quality Certification of an item. This first process is described below:

- (1) One party sends an item **QCertify(X, I)** to the server;
- (2) The server receives the item and sends it to the Quality Certification process where an internal function will be applied. The outputs of this process are (i) the quality description which gives as much detail about the item as possible, (ii) the Quality number;
- (3) When the Quality number is ready, the Quality Certification process sends the Quality number and the item to the Confirm process;
- (4) Confirmation **QCertified(QS, [I, Q#]_{QS})** will be sent to the requesting party signed by the Quality server's private key. This confirmation could be a negative confirmation if the server cannot qualify it.

The second service verifies that a Quality number corresponds to a given item via the following process:

- (5) One party sends a request for quality evidence **VerQty(X, I, Q#)** by supplying the item and the Quality number;
- (6) The server receives the request and sends it to the Compare-Q# process;
- (7) Compare-Q# process sends the item to the Quality Certification process;
- (8) The Quality Certification process certifies the item and replies to the Compare-Q# process with a Quality number;
- (9) The Compare-Q# process compares the number received with the number from the request and sends the result to the Confirm process;
- (10) The Confirm process sends the result of comparison **QtyVer(CS, [I, Q#, Stat]_{QS})** to the requesting party with the item, the supplied Quality number and the status of the comparison signed by the Quality server's private key.

Each item that has been certified should be published by the Quality server, thus providing a complete description of the item in question. The degree of detail regarding the item is what will distinguish between levels of Quality servers. This is also what potential customers will be interested in since it will provide a clear and comprehensive (and therefore more trustworthy) description of the item under consideration. For hard products, e.g. a Toshiba laptop, this could comprise merely the Model number and could be built into the company's own website. For soft products, e.g. a piece of music produced by Sony, a comprehensive specification could also be built into the company's website, based on those features that are considered by consumers to be the most important.

This Quality server idea is a new idea that will be discussed more in section 7.8 to provide further insight into it and the benefits that can be derived from it.

7.7 E-Commerce Transaction Protocol

7.7.1 Notations

Px : Party x who wants to exchange something with the other party **Py**.

Ix : Item x that Px has and wants to exchange.

Qx: Quality of the item Ix [Quality Number].

Cx: Number of Items Ix that Px wants to exchange in a single transaction.

Ax: Delivery Address of the other party where Px will deliver.

Tx: Time interval within which Px will deliver his Ix to the other party.

Sx: The Satisfaction level Px promises the other party [0 or 1].

Exy: The Exchange, transaction or order ID that should be unique in every exchange and should be sent by both parties to the contact server.

Cxy: The Contract between Party x and Party Y and it contains the following (Px, Ix, Qx, Cx, Ax, Tx) and (Py, Iy, Qy, Cy, Ay, Ty)

7.7.2 Assumptions

A1. It is assumed that the channels between any of the TTP and the customer or the merchant are resilient;

A2. The actual exchange of messages will be intense and will involve several rounds. However to illustrate the point, for the sake of simplicity, high level business messaging exchange illustrating only one message will be used. Many of the fair exchange and non repudiation protocols discussed in Chapter 3 can be used when implementing these exchanges;

A3. The Contract and Quality servers are trusted by both parties and the Delivery server is trusted to the party who has used it as a Delivery server;

A4. Servers never crash or they have a crash recovery procedure;

A5. In each server the operations or functions that have direct relation with the transaction itself or the dispute case in question are mentioned. Other operations with no relation to the transaction or the dispute case such as user management in the Delivery server are not of concern here.

A6. Every party can choose a Delivery server that is trusted and from **Ax** it is possible to find the Delivery server, where **Px** will deliver to. For example if the address of the other party is Py@deliverme.com then the Delivery server is Deliverme. Even though it looks like an email address, it does not have to be. For example, where an address is P. O. Box 2425, London SW1BT3 , this can be written as Py@POBox2425LondonSW1BT3 so the Delivery server in this case is **Py** local post office.

A7. Quality server will provide the parties involved in the exchange with a certificate of quality for item concerned.

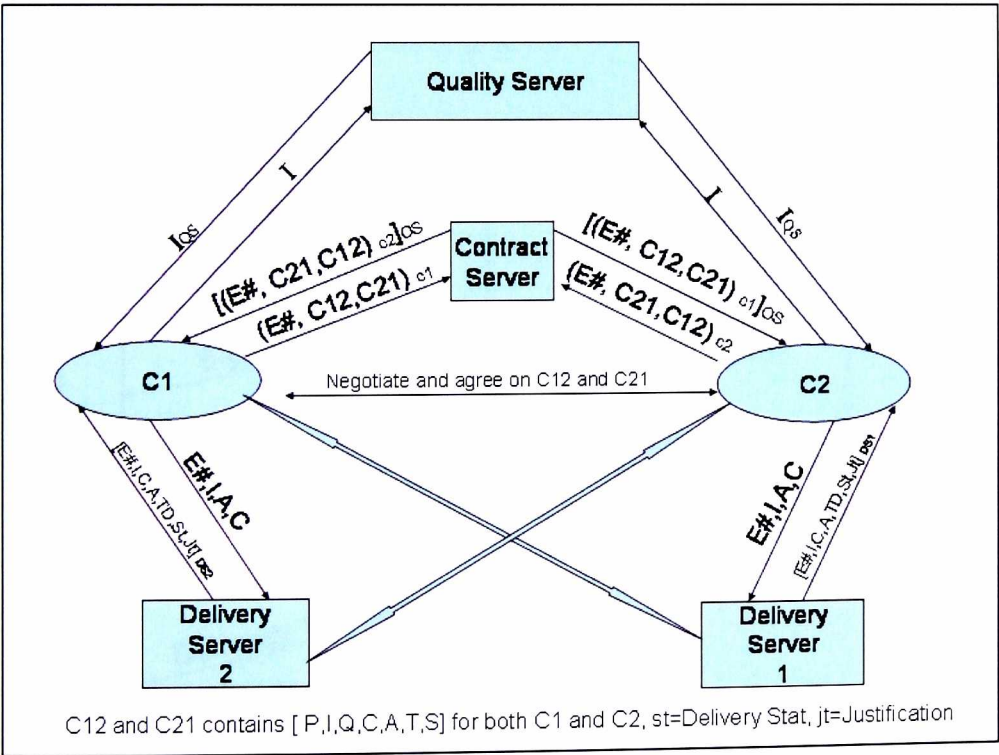


Figure 7-5: E-commerce Transaction Protocol Architecture

7.7.3 Transaction Protocol

To illustrate Figure 7-5 and how the transaction protocol will work, the following is a hypothetical exchange process involving parties (A) and (B) who want to exchange items (IA) and (IB):

Stage1 Involves negotiation and subsequent agreement on all the contract terms;

Stage 2 requires that both parties concerned send the contract which include the following information to the **Contract server**: (E_{AB})(P_A, I_A, Q_A, C_A, A_A, T_A, S_A) and (P_B, I_B, Q_B, C_B, A_B, T_B, S_B)

Stage 3: The Contract server makes sure that the contracts sent to it match and then log the information and ask the two parties to start the exchange.

Stage 4: Immediately after the party receives the confirmation from the Contract server, they will send the item to the Delivery address of the other party.

Final Stage 5: The Delivery server sends a confirmation to the sender and notifies the receiver to contact the Delivery server and ‘consume’ the item.

Figure 7-6 shows the time chart for the protocol.

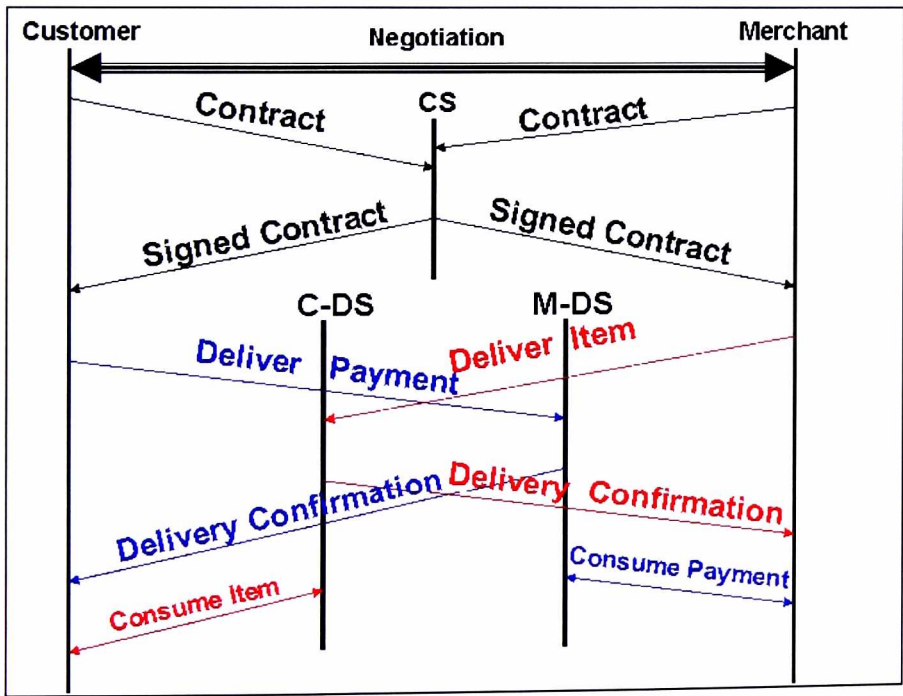


Figure 7-6: Time Chart for the ETP

7.8 Soft Product Quality Certification

The development of e-commerce has been very instrumental in changing the nature of trade; face-to-face transactions are becoming obsolete since more exchanges are conducted online. This new technology is also changing the nature of the products being purchased, and has led to the introduction of soft products i.e. those that can be purchased without shipment and its associated costs, into the marketplace. Items such as software, music and phone calling cards (calling time) [16] are forming a major part of a growing new market, but as a direct consequence, levels of fraud transactions for such products have also increased, and at a faster level than those for tangible products [105]. One of the most significant reasons [25] for this particular increase is that soft products often lack precise description about what is being purchased. For example, whilst buying a piece of music may sound simple enough, the sound quality or production might not be up to expectation. Therefore this section describes a proposed new method of assigning a quality endorsement in the form of a certificate to every possible soft-product via a “Quality server” so that before any purchase is made the specification i.e. quality, can be checked to ensure that this is the exact item required. Where disputes subsequently arise, the party resolving the dispute will compare the actual item received with the quality certificate in order to determine what kind of ‘fair’ resolution is warranted.

7.8.1 The Need for Quality Certification

Most hard, i.e. tangible, products are manufactured according to precise quality and supplier specifications. In consequence, the place of purchase, whether website, printed catalogue or retail outlet, will not affect the item being purchased, particularly where it has been assigned some recognizable Model/Make number and/or a brand name. The same system applies to books via the ISBN number.

However, in the case of soft products, no such mechanism exists [74], and although, for example, in the case of purchasing music, the title of the song and the artist might be the same for every purchase made, other intangible issues such as the location of the recording, production and sound quality might differ considerably. As a result, many potential purchasers are wary of entering into transactions on the Internet and where

exchanges have taken place but have led to dissatisfaction, subsequent difficulties in resolving disputes might be experienced. Invariably this is due to the inability of both parties to agree predetermined and precise specifications before the purchase is made [18].

7.8.2 The Quality Server

Thus the concept of a 'Quality Server' is proposed as a mechanism to try and resolve these kinds of issues. In essence, the Server will receive the soft product, create precise specifications for it and subsequently provide a Quality Certificate. At the same time, the specifications of the item will be published on the Quality server website. Section 7.6 demonstrated how the Server works. In brief, the Quality servers would be designed to provide two main services: Quality Certification of the Item and Verification that the Quality Certificate corresponds to the item in question.

7.8.3 The Quality Certification Process

Having described the general architecture of the server in section 7.6, the actual certification process is now discussed. The method described is only one of many and could be changed according to the demands and nature of the product in question. Every Quality server could have its own method but should still conform to the standard process described above.

Any soft product being purchased will arrive at the server as a stream of bits. Taking as an example 'Song.mp3', the quality certification process would run a hash function on the file and generate a unique 128 Bit number. (This could be longer or shorter depending on the server itself and the nature of the product). The generated number, along with the id of the Quality server, will constitute the Quality Certificate, in the form of (QS, Q#).

The quality certification process will also include writing a complete and comprehensive description about the item and publishing it in a public place such as a website. Currently the process is only likely to be done manually since an expert is needed to make decisions about these factors, but future research will look into developing a framework where this

process can also be automated, especially with known soft-products such as music and software.

7.8.4 Benefits of Quality Certification

Many benefits will accrue from having a unique certificate for each soft product. Prior to purchasing any item, the potential customer will be able to check its description and full specification. From this, the buyer will have complete knowledge of the product they intend purchasing. Searching for a soft-product should be very simple, implying that the auction's automated bidders should benefit and could therefore bid in any of the five hundred auction sites without fear of mismatching the type or item.

From the merchant's point of view, certification of soft products will encourage customers to purchase from that particular point of sale since levels of trust will be raised. In addition, it will facilitate having a trusted party who will be able to decide if two soft products are identical or not, and whether the item being sold was as good as advertised.

In the case of a dispute, the resolving party should be able to make a judgment based on specific product criteria rather than mere speculation as to the nature and content of the item in question. As a result the outcome is likely to be deemed fair to both parties.

7.8.5 Commercial Application of Quality Certification

Having discussed the concept of the Quality server's architecture in the abstract, describing its application in a commercial environment is now appropriate.

Soft products mainly come from two sources. The first is that of commercial suppliers who use professional tools and methods, e.g. Sony Inc which produces thousands of soft products annually. The second is the individual who will create their own product, e.g. a budding artist of some kind who wishes to record and sell his own song, piece of poetry or novel[18].

These two sources of supplies could lead to two kinds of Quality servers: those that are 'private' in the sense that they belong to professionals or large corporations, and those considered 'public', i.e. that would be able to quality anything for the masses.

Sony for example could use its own Quality server and release the certificate with every soft product they create. The cost would be minimal and should not be added to the price of the item. Public servers could provide this service for a small charge, so individuals who create their own products and want to sell them could send their products to these public servers together with the description. The server side could then ensure that the product descriptions were comprehensive and accurate and then subsequently issue the certificate. Even though there would be a charge for this certificate, it would increase the sales of the product since people would now know exactly what they were buying and endorsement by the Quality servers would further increase their level of trust.

Sony would then be able to publish a clear description of the item in its website. Using a song as an example, the title, artist, date, location, sound quality, length, etc. should be specified. If a dispute arises due to a piece of information knowledge that was not clearly mentioned in the description, this omission should then be incorporated into all current and future certification to eliminate future potential disputes. In the long term this should result in a comprehensive description being provided that will eliminate almost all dispute possibilities. There should also be an international standard description for each type of soft product, so that newly created servers could benefit from such knowledge. This standard should provide a comprehensive framework for the item's specification and description.

The issue of Digital Rights Management (DRM) is currently very topical, given the huge number of soft products being created every day. In most existing DRM systems architecture, and in accordance with industry practise, customers use relevant consuming applications that enable them to transact with the licensing and reference services. The licensing service provides a valid source of reference for the correct soft product and its distribution sources. Licenses are generated using the packaging service. Customers also interact with download services designed for the acquisition of soft products that are protected by these licenses. Usually the license must contains the usage rights, meaning that the devices that will eventually play or run the soft-products being purchased are able to check the authenticity of the file and answer the question as to whether or not it is allowed to be played on the device in question.

Adding a Quality Certificate to the DRM architecture as part of the license, or incorporating it as a separate piece of information, will enhance DRM. Devices themselves may prevent files from playing (even if both the device and the soft-product have the correct permission), if the item ordered is deemed not to correspond to that ordered or purchased. Having a quality certificate embedded inside the license of the product itself will ensure that the product license has the correct identity. In this way Quality Certification will provide the best means of identifying the soft product; at the same time the certificate itself can incorporate other information and ensure that the DRM functions correctly.

7.8.6 Quality Certification's Further Research

Soft products suffer from the lack of clear description or quality. This problem affects the development of the soft-product industry and makes customers feel reluctant to buy such items. This section proposed a method of assigning a quality certificate to every single soft product. In reality this is akin to the ISBN numbering system for books and digital certification systems for websites [77].

One problem could be the difficulty of doing such things in real life, however, the answer to such claim is that most soft products are created by commercial firms that if they felt the need for such service, they could adopted it very easily and smoothly. In addition, implementing such architecture is easy due to the maturity of digital certification [64].

It is felt that further research could be directed to this area of e-commerce, and in particular in trying to find electronic methods to eliminate or resolve reasons for disputes in e-commerce transactions.

7.9 Conclusion

Since, as stated at the beginning of the chapter, research has proven that the only truly effective way to lower the cost of resolution is to automate the entire process, the intention of this chapter was to describe a new e-commerce transaction protocol that would be needed to facilitate this kind of development. The current infrastructure was deemed inappropriate due to the fact that even though the Internet was originally built on

trust, this has almost been lost due to cross border transactions and the financial benefits that have been derived from these fraudulent transactions and the influx of soft-products and their associated problems.

This thesis proposed a complete solution in order to solve this problem. This solution consists of two parts: (i) an E-commerce Transaction Protocol (ETP) that was practical and expandable to accommodate any new improvements in the future, and (ii) an Automated Online Dispute Resolution (AODR) system that would automatically resolve any dispute happening within the proposed e-commerce protocol.

This chapter discussed e-commerce transaction protocol in general, its components and how it works. The terminology used was already well-known and the intention was not to create a new technology, rather its intention was to build upon existing knowledge by modifying and suggesting improvements to better satisfy technical needs. At the same time it proposed the need to assign quality certification to soft-products in order to provide purchasers with a precise specification of the item they were purchasing. It would also allow them to refer to the descriptive framework if there was any need for redress.

The next chapter will discuss the Automated Online Dispute Resolution (AODR) system in more detail and show how using the ETP will make it possible to resolve disputes automatically and with minimal cost.

CHAPTER EIGHT

Automated Online Dispute Resolution (AODR)

CHAPTER EIGHT

Automated Online Dispute Resolution (AODR)

8.1 Introduction

Most Online Dispute Resolution Systems are not strictly ‘online’ as discussed in chapter 6 because of the need for human involvement in each process. This is time consuming and costly and now, having explained in the previous chapter how the E-commerce Transaction Protocol (ETP) works, the existence of an effective Automated Online Dispute Resolution (AODR) system, its dependence on an effective ETP, and how the system itself actually functions, is discussed in this chapter.

The AODR is a basic system that, in its own right, is not able to resolve any dispute. Nevertheless the process itself should be able to provide a resolution regardless of the product type and payment method used if it is configured correctly. In order for the AODR to resolve any dispute, a product/payment specific plug-in (add-on) should be incorporated into the system since different product/payment combination result in different dispute types.

Since the focus of this thesis is about disputes regarding soft products and in order to demonstrate how the AODR will work in practice, one of the most common payment methods used in e-commerce, that of using credit cards, has been selected. Therefore the appropriate plug-in specification for soft products and credit cards will be proposed.

The system specification that will be outlined is designed to resolve any type of dispute that could happen in the online transaction system (assuming that the dispute Initiator follows the guidelines accompanying the specification).

8.2 What is AODR

AODR is a system that is claimed to be able to ‘automatically’ resolve any dispute that happens in soft-product transactions given that, if needed, the following data can be provided:

- Order details: obtained from the Contract server by supplying the exchange ID, either or both of the two parties can supply this;
- Delivery certificate: both parties must be able to provide their delivery certificate showing that they did deliver the item as promised.
- Quality certificate: the party being accused of not providing the correct quality should provide this certificate. In certain cases both parties may need to provide this.

AODR has two roles, one is giving advice to exchange participants in order to provide protection from any possible dispute. This advice will come in the form of suggesting good reputation Contract, Quality and Delivery servers and is designed to give protection from fraud when using them in the transaction process. In order for a TTP server to be qualified with the AODR, it must have already shown certification capability and be considered reputable. The second role of the AODR is obviously resolving the disputes.

8.3 Motivation for AODR

8.3.1 Fairness

Fairness is an important feature and actually the most important feature in any dispute resolution system. Most systems that have human involvement cannot guarantee fairness since human feelings and prejudices are not the same in every individual and, as such, cannot be controlled.

The automatic nature of the dispute resolution process will enhance the fairness since machines will work strictly according to the facts and evidence available. Even if

someone who is not guilty is deemed to be so due to a lack of appropriate contradictory evidence, this will be considered fair since an opportunity for them to prove otherwise will have been provided.

8.3.2 Personal privacy

Personal privacy is now a big concern to many people. If the data involved is regarding a payment method or any financial matter, then the concern is higher. As stated earlier dispute resolution that involves the human element usually has many privacy problems, since it is very hard to control. AODR is completely automated, which means no one ever will look into the information provided, and most of the time the AODR will require evidence of only some certification, therefore access to unneeded information is protected.

8.4 How AODR works

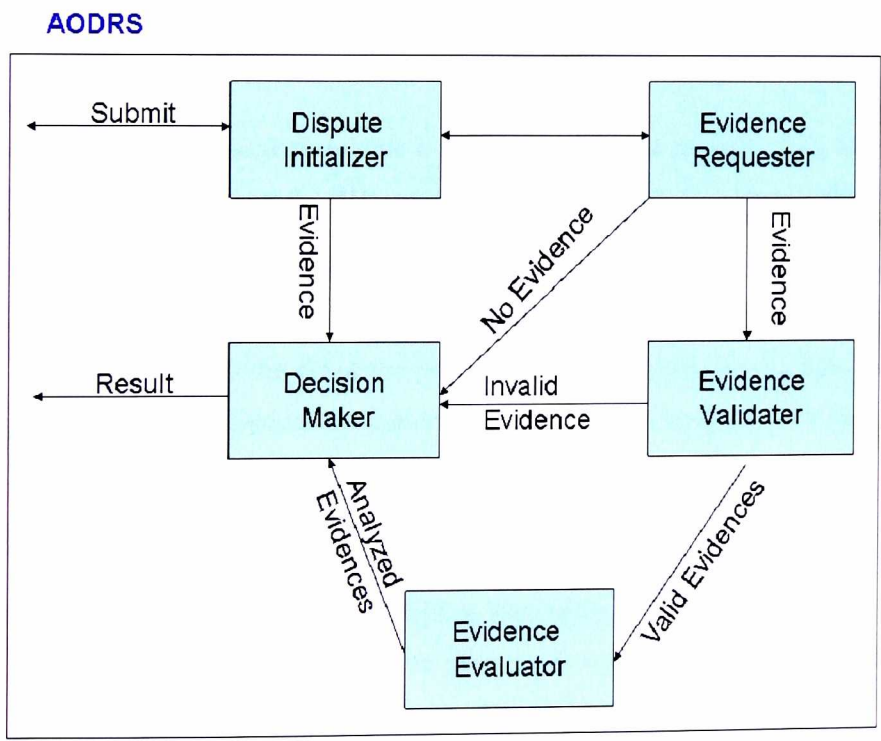


Figure 8-1: The AODR System Architecture

8.4.1 AODR Processes

The following is an explanation of the AODR processes shown in Figure 8-1

Dispute Initializer: this is the process responsible for receiving the dispute from the Initiator and will then provide the interface between the system and the users when evidence is required;

Evidence Requester: this process gets a dispute and subsequently extracts and requests the evidence required;

Evidence Validator: this process ensures that this evidence is valid and correct;

Evidence Evaluator: this process receives the valid evidence from the Validator and analyzes it;

Decision Maker: this process receives all the analysis and decides the outcome of the dispute accordingly.

8.4.2 Messages

- (1) The Submit message to initiate a dispute can be sent by any of the two parties, it contains the Initiator ID (**IID**) and the Dispute type (**D#**): **Submit (IID, D#)**
- (2) Evidence Request, in this message the system sends a request to one of the two parties asking for specific evidence which will assist in resolving the dispute. This message contains the ID of the party who should supply the evidence and the list of evidence required with a minimum of one piece of evidence: **EviReq (ID, Es)**
- (3) Evidence supply, this message will be the reply by the party to the **EviReq** message with the required evidence: **EviSup (ID, Es)**
- (4) The Result message, this message is sent twice, once to each of the two parties telling them the outcome of the dispute. It contains the ID, the status for the outcome of the dispute (**S**), and an optional justification field that can be used to

give more details about the outcome of the dispute or it could be just left for future use (**J**). The status of the dispute has three possibilities of [Success, Neutral, Failure]. In the case where the dispute outcome was to the favor of any of the two parties the one who wins will get a status [Success] and the other will get [Failure] and if the outcome was neutral and no action should be taken, both parties will get [Neutral] in the status field: **Result (ID, S, J)**

- (5) The advice request message, this message is sent by anybody who wants to participate in an e-commerce transaction. It could be sent by a merchant asking what precautions to take to protect his business from fraud, or by a customer asking for advice on how he should complete the transaction without any problem. It contains the ID of the advice requester, the type of product in the transaction (**Prod**), the payment method which will be used in this transaction (**Pym**), and the role of this party in the transaction, Buyer or Seller, (**Role**). The types of products available so far are either Soft-product or Hard-product but more classifications might come in the future: **AdvReq (ID, Prod, Pym, Role)**
- (6) The Advice supply, this message is sent from the AODR to the sender of the **AdvReq** message. It contains the recipient ID and a list of tuples, each of which contains the required evidence and the relevant provider if one is available. For example it should return a message saying that a contract certificate is needed for such transaction and contract.com is a trusted party who can provide such certificate: **AdvSup (ID, [certificate, provider(s)])**

8.4.3 Services

The AODR system provides two main services. The first service is to resolve a dispute and the second one is to provide recommendations to the participant before the transaction. The type of the first message sent will specify which service is requested.

8.4.3.1 The Dispute Resolution Service

This is the most important service offered by the AODR. How it works, is by assuming that there are only two parties in the dispute: the Initiator and the Responder. (Future

research can look into the possibility of their being more than two parties involved in the dispute).

- (1) The Initiator - who is the one claiming that he was cheated- would submit a new case with the AODR **Submit (IID, D#)**.
- (2) If the Initiator does not know the dispute type, he/she will complete a dispute form answering a series of 'yes/no' type questions in accordance with the dispute possibilities mentioned earlier in the taxonomy. For example, it may query whether any item had actually been received.
- (3) After submitting the dispute type or the dispute form, the Dispute Initializer processes it then sends it to the Evidence Requester process.
- (4) The Evidence Requester process produces the required certificate(s). The process is selective and will not ask for every piece of evidence since some may not be available or relevant to the dispute case in question. For example, a quality certificate will not help in a dispute regarding a delivery problem. So the AODR will require only those certificates needed according to the input **EviReq (ID, Es)**.
- (5) After the required evidence received **EviSup (ID, Es)** it will be forwarded to the Evidence Validator process to make sure that these pieces of evidence are genuine.
- (6) If the required evidence is not supplied within the time set by the AODR or the evidence is fake, the information will be forwarded to the decision maker process that will tell the Initiator that the dispute has been rejected.
- (7) If the pieces of evidence are genuine, they will be forwarded to the Evidence Evaluator to review the certificate(s) and make sure that the claims are valid and check if any further pieces of evidence are required from the Responder who is being accused of cheating.
- (8) If evidence is required from the Responder then it will go through the same process as the evidence from the Initiator and then it will be analyzed by the Evidence Evaluator process.

- (9) The analysis of the evidence by the Evaluator will be sent to the Decision Maker process to come up with the decision.
- (10) The Decision Maker process makes the decision and prepares the messages to be sent to the two parties as a result of the dispute **Result (ID, S, J)**.

Figure 8-2 shows the time chart for this service

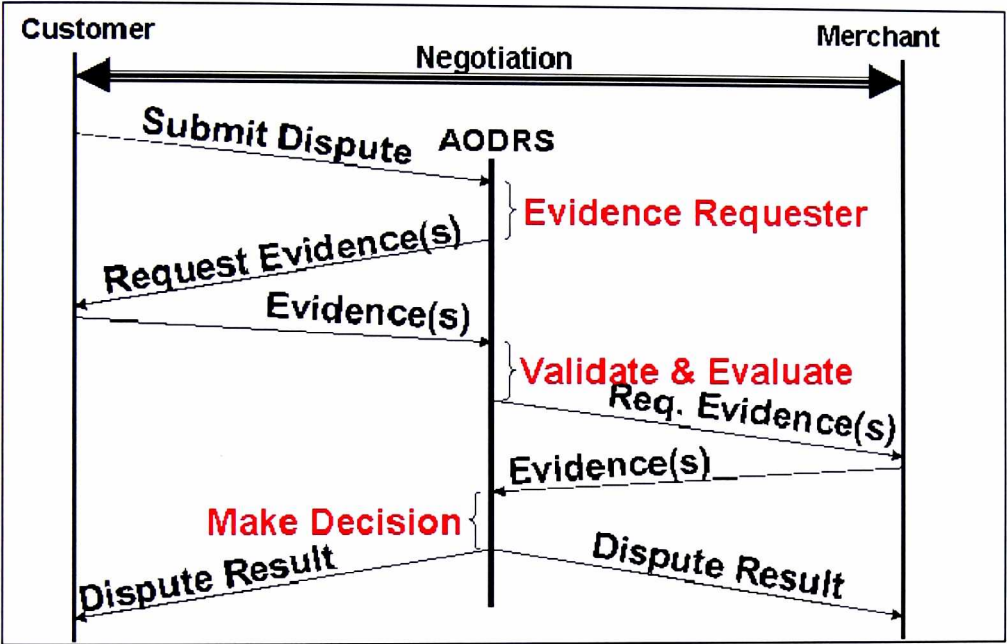


Figure 8-2: Time Chart for AODR Dispute Resolution Service

8.4.3.2 The Advising Service

The second service offered by AODR is advising the e-commerce party, whether customer or merchant, of what precautions should be taken to guarantee a fair dispute resolution. This service operates as follows:

- 1) One party sends a request for advice **AdvReq (ID, Prod, Pym, Role)** by supplying the type of product to be exchanged plus the type of payment method used and the nature of his role in the transaction

- 2) The system replies to the advice requester with all the possible required evidence and some recommendations of who could provide such evidence **AdvSup (ID, [certificate, provider(s)])**.

The idea of this service is that it will tell Internet users what to look for when they want to do any transaction on the Internet. It is also designed to help users protect themselves in their choice of trusted services.

8.5 AODR Plug-in

Having explained AODR process, the rules of the system when making decisions according to each situation will now be outlined.

As previously stated, this system is product/payment specific, therefore every combination will have different resolution. An Add-on or Plug-in for each of these possibilities will need to be created. This plug-in, when compiled, will allow the AODR to resolve any dispute regarding these types of cases.

There are two things to do to create a plug-in for the system. First, all the possible disputes should be analyzed and counted by running the payment method over the E-commerce dispute taxonomy which was introduced earlier in chapter 5 to come up with a set of feasible dispute cases. Second, the associated evidence required to resolve each valid dispute will be identified.

The following are the steps required to create the plug-in for the credit card payment method (see chapter 2, 2.9.3.3 for the credit card transaction cycle).

It starts by listing every dispute possibility, making sure it is possible and could exist using this particular method of payment. It is assumed that Party1 is the customer (Px) and Party2 is the merchant (Py), so Item1 (Ix) is the money and Item2 (Iy) is the soft product needed.

1- Delivery

a. Item1 delivered but Item2 not delivered (DX & ¬DY)

This is the case when party1 pays but receives nothing and this case requires proof of delivery [Delivery Certificate]

b. Item 2 delivered but Item1 not delivered (DY & ¬DX)

This case does not happen since credit card transactions are almost always a 'pay before' transaction, which means you pay first then you get what you want.

c. Item1 not delivered on time (¬TY)

This case does not happen since there is no such late credit cards payment

d. Item2 not delivered on time (¬TX)

The above case requires proof of delivery time stamped and also a proof of the agreed delivery time [Contract Certificate + Delivery Certificate]

e. Item1 cannot be delivered (¬AY)

This case also does not happen since the merchant is the one who will be charging the credit card so it is a pull transaction for him (rather than a push one). If the merchant cannot charge for an item, then it will not be delivered ('pay before' situation)

f. Item2 cannot be delivered (¬AX)

The above case is more complicated than the earlier ones and it requires proof of attempt to deliver [Delivery Certificate].

2- Order:

a. Party1 claims never agreeing to an exchange (¬Px)

This case requires proof of participation in the ETP protocol. This proof can be derived from the proof of agreed terms [Contract Certificate]

b. Party2 claims never agreeing to an exchange (\neg PY)

This case also requires proof of participation in the ETP protocol. This proof can also be derived from the proof of agreed terms [Contract Certificate]

c. Item1 quantity is not correct (\neg CX)

This case requires proof of delivery to show how many were delivered and also proof of agreed terms [Contract Certificate and Delivery Certificate]

d. Item2 quantity is not correct (\neg CY)

This case also requires proof of delivery to show how many were delivered and also proof of agreed terms [Contract Certificate and Delivery Certificate]

3- Item

a. Item1 not Received as agreed (\neg IX)

This case cannot happen if credit cards are used as the method of payment since it is a 'pay before' method, allowing the merchant time to check the validity of the card before sending the item.

b. Item2 Received not as agreed(\neg IY)

This case requires proof of delivery and agreed terms concerning the item being delivered. [Contract Certificate, Delivery Certificate]

c. Quality of Item1 Received not as promised (\neg QX)

This case cannot happen in a credit card situation due to the aforementioned 'pay before' method. Again the merchant can check card validity before sending the item.

d. Quality of Item2 Received not as promised (\neg QY)

This case requires proof of delivery to show what was delivered, proof of quality to demonstrate unacceptability, and also proof of the original terms of agreement

regarding quality etc. [Contract Certificate, Quality Certificate and Delivery Certificate]

e. Item1 received not as expected ($\neg Sx$)

This case cannot happen with the credit card method for the 'pay before' reasons described earlier. .

f. Item2 Received not as expected ($\neg SY$)

This case requires proof of delivery of the item in question, and also proof of agreed terms confirming pre-agreed satisfaction level [Contract Certificate, and Delivery Certificate]

The level of satisfaction should be agreed on before the transaction and can vary from [0-1], where 0 = no satisfaction guaranteed at all and 1= satisfaction is fully guaranteed and the guarantor will pay all expenses if required.

g. Item1 consumed more than once ($\neg MX$)

This could happen easily in with credit card transactions since the merchant will still have the credit card number even after the transaction has been completed and could charge the card an unlimited number of times as long as it has not reached its upper limit. This case requires proof of delivery showing that the credit card has been charged more than once for the same order and the agreed terms [Contract Certificate, and Delivery Certificate]

h. Item2 consumed more than once ($\neg MY$)

This case requires proof of delivery showing that Item2 was delivered more than once for the same order and the proof of agreed terms [Contract Certificate, and Delivery Certificate]

Having analysed alternative outcomes of using the credit card as a method of payment for a soft-product, with the dispute taxonomy previously described, a list of possible disputes has now been compiled using the following format

(D#) {(Dispute reason, [Evidence required]}:

(D1) {Item1 delivered but Item2 not delivered ($Dx \ \& \ \neg Dy$) [Delivery Certificate]}

(D2) {Item2 not delivered on time ($\neg Tx$) [Contract Certificate + Delivery Certificate]}

(D3) {Item2 cannot be delivered ($\neg Ax$) [Delivery Certificate]}

(D4) {Party1 claims never agreeing to an exchange ($\neg Px$) [Contract Certificate]}

(D5) {Party2 claims never agreeing to an exchange ($\neg Py$) [Contract Certificate]}

(D6) {Item1 quantity is not correct ($\neg Cx$) [Contract Certificate and Delivery Certificate]}

(D7) {Item2 quantity is not correct ($\neg Cy$) [Contract Certificate and Delivery Certificate]}

(D8) {Item2 Received not as agreed ($\neg Iv$) [Contract Certificate, Delivery Certificate] }

(D9) {Quality of Item2 Received not as promised ($\neg Qy$) [Contract Certificate, Quality
Certificate and Delivery Certificate]}

(D10) {Item2 Received not as expected ($\neg Sy$) [Contract Certificate, and Delivery
Certificate]}

(D11) {Item1 consumed more than once ($\neg Mx$) [Contract Certificate, and Delivery
Certificate]}

(D12) {Item2 consumed more than once ($\neg My$) [Contract Certificate, and Delivery
Certificate]}

After generating the dispute IDs as above, the Resolution Procedures will be added to each case. So the plug-in created will have the following format

(D#) {(Dispute reason, [Evidence required], Resolution procedure}.

This plug-in can then be fed into the AODR and should then be able to resolve all dispute cases if the item is a soft products and the payment method used is a credit card.

It should be stressed that this plug-in is only designed to show those dispute cases that can be resolved by the AODR system. System providers, when implementing it, should write the code for the Resolution Procedures to resolve each case according to the given dispute type.

This plug-in will be used in the dispute resolution service. The type of certificates used in this plug-in are those that should be used in the second service in supplying advice to the participants. Trusted Third Parties in the ETP should register with the AODR providers to be recommended to customers.

It has not been within the scope of this thesis to go into great detail about coding the Resolution Procedures: future research should look into this in more detail. For simplicity and because of time constraints, it has been enough to confirm that the certificates are genuine and compatible in order to be able to come up with the appropriate resolution. For example the Resolution Procedure for Dispute1

(D1) {Item1 delivered but Item2 not delivered ($Dx \ \& \ \neg Dy$), [Delivery Certificate]

[If Party1 submits a genuine delivery certificate and party2 could not provide one, then Party1 should win the dispute, but if Party2 submits a genuine counter delivery certificate, then the dispute is rejected]] and so on for all the rest of the disputes.

8.6 Reasons for the Success of AODR

8.6.1 Implementation Independent

The concept of AODR is merely abstract at the moment; no implementation has yet been available. In the future every AODR provider will be able to implement their own version but should follow the guidelines to be able to offer at least the services described above.

Different providers could subsequently offer more services to attract customers to use their system. Providers should aim to gain a good reputation in order to persuade merchants to participate with them since this maybe optional.

8.6.2 Protection Against Organized Crimes [Professional Hackers]

Organized crimes usually are the most difficult to fight, since hackers know almost everything about the systems in use and their drawbacks. AODR will provide protection from this kind of crime because it uses the ETP which follows a very systematic transaction procedure and also provides the parties involved with the essential evidence.

AODR, when used with ETP, will verify the evidence and make sure that both parties will get a fair resolution. Professional hackers will not benefit much if ETP and AODR are used together and merchants insist that they are used. This is because ETP with AODR provides a strong authentication scheme and many trusted third parties servers are involved, resulting in fair distribution of the responsibilities in the case of fraud.

8.6.3 Time and Resources Optimization:

Usually the ODR systems will contact the Responder as soon as it receives the dispute from the Initiator. This means that some merchants will get many queries to participate in resolving disputes that are not really valid where the Initiator has just simply not read the rules or wants to try and claim compensation from the merchant even where he is at fault. However, the AODR is designed not to contact the Responder unless the claim from the Initiator is valid and the evidence is proved to be correct.

8.7 Enforcing the Result

Enforcing the result is a very difficult and important process in dispute resolution, however what really governs the difficulty and the importance is the party that is implementing the AODR. One good example of such a party might be dispute departments in credit card companies. Currently they make their decisions through manual investigation and phone and mail communications [22]. However their

investigation results are always enforceable on both parties because they have the right to credit and debit both accounts.

8.8 AODR Providers

Funding of the service provider is a general problem with any dispute resolution system. If customers have to pay for the service, it might prevent them from initiating the dispute; if merchants fund it then they will only fund the one who will be in their side in case of a dispute. AODR does not have this kind of problem since the cost is not high due to a lack of human involvement.

There are many good candidates to fund the AODR provider, whether customers paying a minimal charge of e.g. \$1, or merchants paying the same nominal amount for every case filed and heard. Governments should also support the AODR since it will encourage more customers and merchants to benefit from e-commerce without having any reservations.

The choice of the provider should be based on two things, the ability to fund the infrastructure and the ability to enforce the result.

8.9 Enhancing AODR

8.9.1 Limitation of AODR

Current AODR design means that the number of dispute cases that can be resolved is limited. This limitation comes from the fact that each payment and goods type combination will have a different set of cases. This limitation of the cases covered could be removed by either coming up with all the possibilities for the payment and goods type combinations and then trying to generate all the cases, or by trying to abstract the cases into a more generic analysis and then be able to cover all current scenarios.

AODR should be able to compare the dispute case even if the exact payment and goods type does not yet feature in the scenario analysis framework. In this way it should be able to presume the same case and therefore be able to come up with a resolution. Even though the resolution will not be binding since it has made this presumption to come up with the result, it should still be able to give a good indication as to who is right and who is wrong. Therefore the type of products and payments supported should be mentioned clearly on the AODR provider's website.

Hard products face one important problem of comparing the item ordered to the one delivered: AODR systems will not be able to make this comparison and so will not be able to resolve the dispute. However, this problem could be solved by funding private or government agencies that would make offline comparisons and then send evidence electronically to the AODR which will then make a decision as a result of the inputs it has received.

These agencies would compare the item and note the comparison result in the same way that banks would make photocopies of e.g. passport originals and it will substitute the Quality server in the ETP.

AODR providers may ask for different evidence and also the trusted third parties may offer the evidence in different formats, as a result this inconsistency may jeopardize the AODR from being able to resolve the dispute correctly. There should be a standard body that will issue a clear specification of the type of evidence needed and the content required from each piece of evidence.

ISO would be an ideal body to undertake this function but it will probably take quite a long time to come up with a standard – by which time many providers are likely to be working to their own proprietary systems, making any modifications required for standardization difficult to implement.

The suggestion here would be to submit to the ISO a complete draft with all possible certificates and contents in order to expedite the process and make the draft available to the public so all the providers would have a common base from which to start.

8.9.2 Reducing the Involvement of TTPs

As discussed in chapter 7, the ETP needs three TTPs to be involved in the transaction to make sure that both parties will get a fair resolution where disputes arise. The involvement of the TTPs depends heavily on the current technologies available to authenticate and verify the information agreed and exchanged.

For example, if the asymmetric cryptography infrastructure is available and if both parties have private and public keys then a good improvement to the ETP would include removing the Contract server completely. Both parties would sign the contract by their private keys and send it to the other. When received they would use the other party's public key to read the contract and make sure it corresponded to what was being agreed. When a party decrypts the contract by the other party's public key and subsequently finds that the contract matches what is being agreed with, the delivery can be immediate since this will be enough evidence of participation and agree terms.

Future technologies may allow the ETP to get rid of all the TTPs in the future; this is something worth more investigation and future study.

8.9.3 Reducing Storage Requirements for the Users

The cost of resolving a dispute using the AODR should be minimal since this is the major aim of such a system and no human element is involved. The hardware cost will affect the overall cost significantly. Some dispute cases will involve evidence where the item itself is a soft-product, or some parts of the item are embedded in it which implies that a great amount of storage space is needed, resulting in higher hardware cost and an even higher resolution fee.

The AODR will sometimes request more evidence from both parties during the resolution period. Parties may not respond immediately, in consequence the whole case will need to be saved until the evidence arrives. The time of arrival of the evidence will usually be unknown, meaning that even more storage space will be needed to store cases still being processed.

Resolved cases will sometimes be needed at a later stage, especially if the enforcement is done through a different body. Archiving the resolved cases will also require more disk space.

Some actions can be taken to try and minimize the need for disk space. For those cases currently being processed the evidence size could be minimized by using the hash of the item rather than the actual one. This could be generated by the TTP. If not, then the AODR can take the item, hash it and then delete the original to save space.

For those cases pending and waiting for evidence, there should be a reasonable enough timeout before the AODR considers that the party is not willing to submit the evidence or it is not available. This amount of time should not be too short, it should give parties adequate time to submit their evidence; it should also not be too long, so that the system does not need to store too many cases. The party that is required to submit evidence should also be allowed to ask for an extension or be able to reply saying that the evidence is not available.

A timeout period should also be specified for resolved cases. This period should be long enough so that the enforcement is able to take place within it. Parties involved in the resolved dispute case should have the ability to ask for an extension of storage before it is deleted. They should also be able to confirm to the AODR that the result has been enforced and that the case can be deleted.

8.9.4 Support for Users with No Evidence

In the current configuration of the AODR, if the evidence is not presented, the case will be closed. An improvement on this would be to try to resolve the case by asking for the required evidence and, if not available, requiring that the other party rejects the claim or comes up with counter evidence.

For example in the case of a customer having ordered four items, receiving only three and subsequently claiming that the delivery evidence has been lost, the AODR should try to contact the merchant and explain the situation. The merchant would then be required to check internal records and, on finding the mistake, send the remaining item to the

customer. Although the merchant could not be forced into doing this, it is unlikely that he would want to take advantage of the customer's situation and not comply with the request.

8.9.5 Resolution Outcome

Usually the outcome from the system will involve decisions regarding whether or not to reimburse the customer. However, it could be that the actual amount to be returned is also questionable, in which case some value should be included in the contract stipulating that in the event of a dispute, this is what each party would be required to pay.

Penalty clauses could also be included, e.g. if goods were not delivered on time a nominal amount should be paid, likewise for an under-delivery or failure to comply with other, previously agreed, contract conditions such as quality of service.

8.10 Conclusion

To re-iterate, most Online Dispute Resolution Systems are not strictly 'online' because of the need for human involvement in each process, making them time consuming and costly. However, the proposed AODR in this thesis is verifiably 'online' in its execution, since it is able to resolve any dispute without human involvement. It is designed to work in conjunction with real online transactions where everything is automated, although there could be some exceptions to this if the parties involved in the transaction were able to comply with the requirements and generate the required evidence themselves.

The AODR should provide results for the dispute and, although the concern here has not been about result enforcement, it should make this aspect of the process easier by ensuring the decision making stage is more efficient and effective.

Although the AODR system is only a basic and not able to resolve any dispute per se, it should, as indicated in the introduction to this chapter, be able to provide a resolution regardless of the product type and payment method used if configured correctly.

Therefore the chapter has described the product/payment specific plug-in (add-on) that would need to be incorporated into the system. The system specification that has been described is designed to resolve any type of dispute that could happen in the online transaction system (assuming that the dispute Initiator follows the guidelines accompanying the specification).

The next chapter will talk about a case study of e-commerce in Saudi Arabia which has been used to test the viability of both the e-commerce dispute taxonomy and the proposed model. The case study shows the suitability of using ETP with AODR in order to resolve soft-product disputes automatically.

CHAPTER NINE

E-commerce and E-commerce Fraud in Saudi Arabia: A Case Study

CHAPTER NINE

E-commerce and E-commerce Fraud in Saudi Arabia:

A Case Study

9.1 Introduction

This chapter will discuss the potential market for e-commerce in Saudi Arabia, the current infrastructure available and plans for future infrastructure developments to better support the growing e-commerce marketplace.

During a field trip to Saudi Arabia the following information was collected to describe the current situation of e-commerce in Saudi and to help determine its future. The choice of Saudi Arabia for this study arose from three factors, first: Saudi is a growing market for e-commerce and disputes; second: some important information was needed to be collected to test the proposed protocols in this thesis, and Saudi has less strict privacy rules than the U.K, and finally, the first implementation of these ideas is most likely to be in Saudi Arabia.

The case study was conducted in Saudi Arabia over a 3 month period, between April and June of 2005. The study had 3 main objectives:

- 1) To find out more about the nature of e-commerce and e-commerce fraud in Saudi Arabia;
- 2) To verify that the e-commerce dispute taxonomy generated in chapter 5 of this work was complete and therefore appropriate;
- 3) To study some complex fraud cases and ensure that if the ETP and AODR are used the cases in question would have been easily resolved.

9.2 The Potential Of The Saudi Arabian Market

Despite having 23 million inhabitants and an estimated IT product market of \$6.3 billion in 2004 (with computer sales representing \$850 million), the growth potential for e-commerce has been constrained by the absence of a regulatory environment, slow penetration of the Internet and advanced, i.e. broadband, telecommunications. In 2001 Saudi Arabia represented the Arab world's largest market for IT products with over 33% of its total PC sales. The estimated number of installed bases PCs is over 800,000, however Madar Research [86] puts that figure at nearer 1.5 million [13, 39, 129].

Whilst this number may seem large in volume it is still small in terms of penetration compared to most other countries in the Gulf [13]. With more than \$7.0 billion invested, plans are now being developed to turn Riyadh, the capital, into a major IT and telecommunications centre in keeping with the demands of a growing information conscious society. Whilst the Saudi Arabian government concedes that the country may be considered behind its smaller Gulf neighbours in terms of speed of Internet-related achievements, relative to its size it is still making fast progress towards its goal of universal access to telephony and the Internet [129].

9.3 Current Infrastructure

Universally, E-commerce has three main 'pillars': communication and Internet, payment, and delivery services. These are now described in the context of Saudi Arabia.

9.3.1 Telecommunication and the Internet:

In terms of an infrastructure for e-commerce, telecommunication is the most important. This sector was liberalised by the Saudi government in 2001, opening up the market to foreign investment and therefore competition.

Use of the Internet has been available in Saudi through domestic servers since 1998. In 2001 there were 350,000 users, today that figure exceeds 2.2 million, representing a penetration rate of around 10% of the population [50].

Internet connection fees are considered high although recently the Saudi Telecommunication Company (STC) announced a 25% cut. At the same time new pricing models are being considered by the government and ISPs in an effort to make connection more affordable for users. At the present time, individuals, companies, organisations and government agencies other than universities must subscribe to Internet services through one of only 21 currently licensed ISPs in the kingdom. Universities are allowed to have their own Internet service [50].

9.3.2 Payment Methods:

The Saudi Arabian Monetary Authority (SAMA) is the central monetary authority. In mid-1980s it established the Saudi Payments Network (SPAN), a “neutral” national transaction switch that linked the ATMs of all the commercial banks on a reciprocal basis so that all bank customers could withdraw cash at any ATM in the kingdom. This led to a national ATM service coverage with 2,577 ATM terminals in online daily operation in SPAN.

Currently around 19 million transactions are processed every month with a total value of around SAR 12 billion. SPAN terminals accept Visa and MasterCard transactions (and in the near future they will also accept American Express).

Cheques are cleared at local clearing houses that are maintained at each SAMA branch.

The Automated Clearing House (ACH) accounts for the bulk of cheques cleared at the SAMA three main centres, while remaining cheques are cleared through manual clearings at the other seven SAMA branches [39].

The use of credit cards as a means of payment is not widely used in Saudi Arabia for three reasons. First, Islam prohibits people to take or give (financial) interest and most credit cards work on this basis. Second, most consumers use debit cards (ATM cards), removing the need for credit cards (unless there is a need to be able to access cash internationally). Third, disputes in Saudi involving credit cards usually mean that the

customer will have to put forward the cost of the transaction first and only then will the dispute be investigated and hopefully be resolved in their favour.

In consequence, the number of credit cards as a ratio to debit (or ATM) cards in the country is currently only 1:10 according to a recent interview with a SAMA official.

With specific regard to the focus of the thesis, there are currently no e-payment schemes in operation in Saudi Arabia [39].

9.3.3 Delivery

The Saudi Arabia postal service is still very inefficient. Only one government establishment is responsible for distributing mail to central post office boxes and at the same time sending national and international mail. From a situation in 1998 where there were only 4 P.O. outlets in Riyadh, there are now 400 after it was approved that small private post offices could offer their services [110].

However, even now mail cannot be delivered directly to homes or offices (and can only be delivered to mail boxes). Nevertheless infrastructure improvements are intended to change this situation.

9.4 Future Infrastructure

The Saudi Government is now taking vital steps towards reviewing regulations for e-commerce and planning for e-government. Many banking institutions and large companies have also set up infrastructures for e-commerce in order to maximize the advantages of online business [50]. The following describes how these steps for the future are being developed, again using the e-commerce 'three pillars' concept.

9.4.1 Communication and Internet

Saudi Arabia represents the largest and fastest growing telecoms products and services market in the Middle East. Total expenditure within the sector is expected to reach

\$4.7billion by the end of 2005, and increase to \$60billion by 2020. The Government's latest Telecom Development Plan for the period 2000-2005 aims to increase line density rates to 25 lines per 100 people by the end of 2005 (a huge increase from the 10 lines per 100 in 1996) [50].

Whilst the country has not yet reached a point where voice traffic has been surpassed by data traffic, as with most of the world, its future appears to belong to data and broadband wireless systems. The number of leased lines is expected to grow annually at around 18%, with a further increase to 40,000 by 2006 according to the Telecommunications and Information Technology Commission (CITC). More than \$10billion is expected to be invested in new data information technologies in the country between 2005 and 2020 [50].

Saudi Arabia's e-commerce market is expected to grow from \$1.5billion in 2002 to \$8billion by 2005 according to the latest Madar Research results [86]. There is also a growing demand for network management, data warehousing and web hosting services, along with increasing opportunities in more the traditional areas such as communications analysis, design, control and training subsectors [50].

9.4.2 Payment

Research results from interviews with SAMA officials indicate that the only new development in the payment sector will be that of using the smart card instead of the usual PIN debit card. Their opinion is that this will help boost the portability of payment and lead to further market penetration in card use. At the same time it is hoped that use of smart card readers will further facilitate and help increase e-commerce transactions due to increased levels of trust in security.

Credit cards should also have more acceptability since SPAN terminals now accept Visa and MasterCard transactions (and in the near future will also accept American Express).

In the first quarter of 2005 there was a substantial growth in online purchases by online domestic and international Visa cardholders using the Internet, transaction business was valued at over \$100,000 during the period [138].

Early 2004, the Samba Financial Group became the first e-commerce acquirer in Saudi Arabia and was closely followed by the launch of their Internet payment service 'SambaConnect' (e-commerce 6) [138].

The CEO& MD of SAMBA (and also Visa CEMEA board member), is quoted as saying:

'With SAMBA providing the solutions for online transactions as the only e-commerce acquirer in the Kingdom, we have witnessed increasing acceptance of online purchases. We expect greater online activity in the coming months as more merchants in Saudi Arabia begin to take advantage of this delivery channel and offer online purchase facilities, which are fully protected by Visa International's latest e-security programme, 'Verified by Visa', in addition to the security benefits offered by SambaConnect. With large acquirers such as Saudi Arabian Airlines now offering online payments through SambaConnect, there will be a further deepening of the market' [24].

9.4.3 Delivery

In 2005 the Saudi Post approved a project to begin delivering mail to houses and expected to distribute around 5 million boxes in this project. The intention is to deliver mail in a timely manner direct to houses using latest technology smart P.O. boxes linked to satellites and postal trucks, and using the GPS to find addresses correctly.

E-commerce merchants will, as a result of this project, be able to deliver goods directly to houses, increasing levels of trust in the transaction system as a whole and ensuring that the items ordered will go directly to the payee's registered address rather than the previous PO Box number used previously.

This will facilitate using some verification systems similar to those used in the USA or Europe to make sure that the payment method used belongs to a specific address, an example of such a system is the Address Verification System (AVS).

9.5 E-commerce and Fraud

To re-iterate, Saudi e-commerce is only conducted via the use of credit cards and the next section will examine fraud cases in this area. SAMA officials rely on information from the major credit card companies about the security of their cards.

The General Manager of Saudi Arabia Visa International commented that: 'The rising number of transactions is an indication of the growing comfort level of Visa cardholders when they make online payments. At Visa, we are committed to providing a secure online payment environment to consumers through constant innovation of new technologies. Our e-security program, 'Verified by Visa' is one such example that is promoting peace of mind and trust of cardholders when they shop from the comfort of their home or office at anytime' [24].

The appropriateness of the program 'Verified by Visa' as a security precaution has already been criticised in section 4.6.3 of this thesis. These criticisms were raised subsequently as part of the project's research with Mr. Ian Hudson, GM of Visa CEMEA who, unfortunately, was not able to answer the shortcomings about the system that had been raised.

9.6 Verification of the E-commerce Dispute Taxonomy

The e-commerce dispute taxonomy generated in chapter 5 is the first of its kind. The intention in generating it was to help those parties involved in the field of dispute resolution to better understand the associated problems and therefore better facilitate the resolution process

Completeness in the taxonomy was verified using the Truth Table method. However, for further confirmation the taxonomy was then tested in several live e-commerce dispute cases in Saudi Arabia over a period of one month in one of its major banks. The results are analysed below.

520 dispute cases were monitored during the month, at an average of 18 disputes per day. 257 cases involved use of the VISA card, 263 regarding MasterCard. Customers provided many reasons regarding the nature of the dispute, for consistency these have been summarized in groups according to the nature of the dispute. Table 9-1 shows how the dispute initiators' reasons have been grouped, and the number of disputes related to each type of credit card.

Table 9-1: Saudi Fraud Cases and Reasons

	Reason	Visa	MasterCard	Total
1	Merchant has no authorization	96	160	256
2	Authorization canceled	14	24	38
3	Charged my expired card	6	11	17
4	Transaction not recognized	19	32	51
5	Canceled recurring transaction	3	3	6
6	Paid by other mean	46		46
7	Charged twice	25	19	44
8	Service not rendered	25	8	33
9	Goods returned but not money	5	6	11
10	Item received late	14		14
11	Amount not correct	3		3
12	Incorrect currency	1		1

Although at first sight these reasons may appear to be different from the taxonomy presented earlier in the thesis, the following shows that in fact, all of the cases can be analysed using the suggested framework.

- Reasons 1 to 5 are similar to dispute [2-a] in the taxonomy which is “Customer claims never placing the order ($\neg Px$)” since without proof of authorization there is no proof of participation;
- Reasons 6 and 7 are similar to dispute [3-g] in the taxonomy which is “Multiple Payment consumption ($\neg MX$)” since all these cases mean that the merchant charges the customer more than once;
- Reasons 8 and 9 are similar to dispute [1-a] in the taxonomy which is “Payment received but goods not delivered ($Dx \ \& \ \neg DY$)”;
- Reason10 is similar to dispute [1-c] in the taxonomy which is “Goods not delivered on time ($\neg TX$)”;
- Reason 11 is similar to dispute [2-d] in the taxonomy which is “Amount paid incorrect ($\neg Cx$)”;
- Reason 12 is similar to dispute [3-b] in the taxonomy which is “Received money not as sold ($\neg Ix$)”.

Therefore from the above analysis it is clear that all 520 reasons for the dispute cases are covered by the taxonomy, providing further assurance that the taxonomy is robust and therefore able to cover all dispute case possibilities.

9.7 Validity of the Use of ETP and AODR

The main theme of the thesis has been to develop an automated system to resolve disputes occurring online. The case study found that the major cause of dispute was where customers claimed they did not recognize the transaction, i.e. claiming that they did not place the order. This form of dispute is also the most costly. Table 9-2 analyses dispute reasons, the number of cases involved, together with their total monetary values.

Figure 9-1 shows the results as percentages.

Table 9-2: Dispute Cases and Reasons in Saudi Arabia

Reason		MasterCard		Visa		Total	
		Cases	\$Value	Case	\$Value	Cases	\$Value
1	2-a. Customer claims never placing the order (~Px)	230	78970.5	138	176886.7	368	255857.2
2	3-g. Multiple Payment consumption (~Mx)	19	2605.303	71	90780.57	90	93385.87
3	1-a. Payment received but goods not delivered (Dx & ~Dy)	14	4732.51	30	96700.46	44	101433
4	1-c. Goods not delivered on time (~Tx)			14	13714.83	14	13714.83
5	2-d. Amount paid incorrect (~Cx)			3	11979.11	3	11979.11

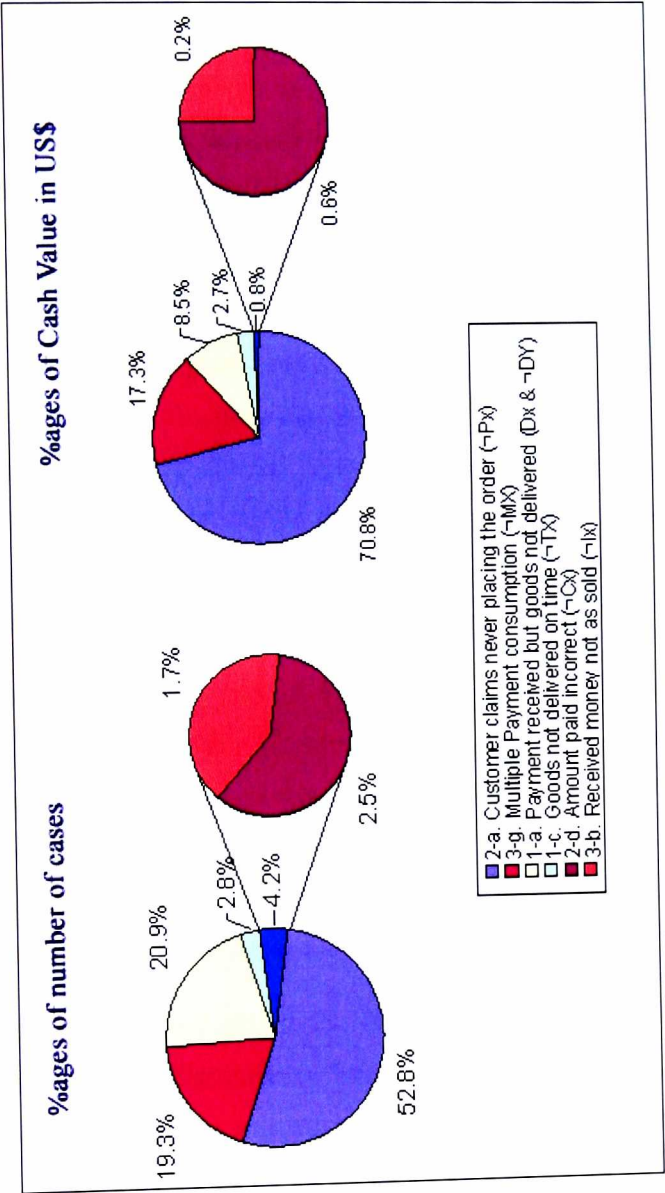


Figure 9-1: Percentages of Dispute Reasons in Saudi Arabia

The statistics show that 52.8% of all cases and 70.2% of all monetary values related to only one type of dispute, the nature of which is a major problem in all soft-products transactions. To re-iterate, this type of dispute is based on claims by the customer that the order was never placed.

The second source of dispute arises from the situation where the item is claimed not to have been received. Together these two sources of dispute amount to 73% of all cases and 79% of all monetary value in the case study. These figures are highly significant and together the two causes of dispute indicate major problems in these areas.

During the period of the case study the resolution process and its outcome was monitored closely. At the end of the period it found that 100% of dispute outcomes favoured the customer since merchants had no proof of any contract or delivery. As a result merchants were forced to return the money back to the customers' accounts. However, in reality around only 18% of these cases provided a fair resolution, since only 18% of the merchants admitted a mistake had been made in charging the customer. In the remaining 82% of cases the merchants rejected the disputes but, since they lacked the necessary evidence, they inevitably lost the case.

Each one of these disputes took around 5 weeks to be resolved. Interviews with merchants, customers and third party dispute resolvers resulted in an agreement that if the Automated Online Dispute Resolution (AODR) system had been available, the resolution time would have been substantially reduced to only 10% of the time currently being wasted on the process. At the same time it was acknowledged that the outcome was not likely to be fairer using the AODR process.

However, all parties also agreed that if the AODR process was used within the e-commerce infrastructure, the E-commerce Transaction Protocol (ETP) also proposed in this work, it would improve the resolution time even further and lead to 100% fair resolution outcomes since every single exchange is monitored and both parties have the required evidence. For example, the dispute case {[2-a] Customer claims never placing the order ($\neg Px$)} will take only one message from the AODR asking the merchant to supply the contract for the transaction, if the time given to the merchant is 3days, then this dispute will be resolved in maximum of 4days instead of the normal 5 weeks procedure. Moreover, if the ETP is also used the result will be fair since the merchant has the contract evidence.

9.8 Conclusion

The case study examined the nature of e-commerce and e-commerce fraud in Saudi Arabia and tested the completeness of the taxonomy and the capability of the ETP and AODR models as a means of providing automatic solutions to the dispute resolution problem.

A series of complex fraud cases were analysed in order to confirm their appropriateness. Saudi Arabia, one of the most significant countries in the world at the moment in terms of Internet and e-commerce growth (and therefore deemed appropriate to test the potential for this new dispute resolution technology) was chosen as the focus for the research.

The nature of e-commerce and e-commerce fraud in Saudi Arabia as one of the leading market with potential expansion were studied. It also verified that the e-commerce dispute taxonomy generated in chapter 5 of this work was complete and therefore appropriate to be used in any design for a dispute resolution system. Finally, the case study some complex fraud cases and confirmed that if the ETP and AODR were used, the cases in question would have been easily resolved.

The next chapter will provide a conclusion to the thesis by summarizing its original objectives, subsequent research and findings that led to proposals for a new solution, contributions to the current field of academic study and suggestions for future research.

CHAPTER TEN

Conclusion

CHAPTER TEN

Conclusion

10.1 Introduction

Despite a growing e-commerce market that still has huge potential for the future, the issue of dispute resolution is beginning to be a major deterrent to its expansion [42]. The increasing number of transactions is also leading to higher rates of dispute and reluctance on the part of many customers and merchants to conduct business in this way. The major concern on both sides is that contractual rights will not be protected appropriately because the dispute resolution system is perceived to neither be robust nor fair.

With regard to soft-products this issue is even more complicated and even further behind in dispute resolution development than that of hard-products since these products are usually small in value, difficult to trace and as a result confirmation of delivery is usually difficult to obtain.

Therefore the objective of this thesis was to develop a system whereby purchasers buying soft-products online and using any e-payment method would also have access to a speedy, inexpensive and equitable dispute resolution system should the need arise.

This was achieved by constructing enough evidence before, during and after the transaction. The result led to the proposal of a solution to this major issue of fraud in soft-products through technical rather than more traditional means, i.e., laws and regulations in a court environment, since it was argued in the thesis that this more traditional approach would not be capable of being enforced in the electronic world and would have no authority in the global Internet environment as a result.

Dispute scenarios from many different perspectives were analyzed, viz. computer science, business, legal and that of the participants themselves. The analysis then led to the design of a comprehensive taxonomy framework for dispute in e-commerce.

The new solution that was proposed was intended to overcome all previous alternatives that still incorporated a human element in the process, since this led to higher, unnecessary additional costs regarding time and eventual redress. This factor was seen as crucial to its success in terms of improving confidence levels in e-commerce since previously the costs of dispute resolution were often higher than the value of the original item under dispute.

The outcome of the research proposed that the online dispute resolution process could be completely automated in two stages as follows:

- 1) an E-commerce Transaction Protocol (ETP) forming the infrastructure where the transaction would take place and be able to accommodate any new improvements in the future,
- 2) an Automated Online Dispute Resolution (AODR) system which would automatically resolve any dispute occurring within the proposed e-commerce model.

The AODR system required a product/payment specific plug-in (add-on). This plug-in would be incorporated into the system to resolve all dispute cases specific to this product/payment type. For illustration purposes, credit cards as a payment method were selected, since this was the method of payment used for approx. 90% of all e-commerce transactions, and an appropriate plug-in specification for payment of soft products by credit card was designed and tested.

The research findings in the thesis should help the whole e-commerce community since they give a whole picture of the solutions without going into details. However, the actual implementation and coding of these protocols is out of the scope of this thesis and could be completed in the future as part of the ongoing research in this field.

10.2 Contributions

The thesis makes the following contribution to the general field of computer science, and e-commerce security in particular:

- It has studied the features of current payment methods in general and then used this general framework to analyse the features of new payment methods;
- Provided suggestions as to how the current state-of-the-art fraud detection and prevention technique, the Address Verification Service (AVS) could be upgraded to a Full Address Verification Service (FAVS) which would be able to detect and prevent fraud that occurs when soft-products are the items being purchased;
- Generated the first e-commerce dispute taxonomy in order to provide an adequate basis for dispute resolution system designers and others dealing with resolutions per se in order to better understand the nature of the online environment;
- Proposed an E-commerce Transaction Protocol (ETP) as an infrastructure for e-commerce which would guarantee that both parties involved in the transaction would have enough evidence in the case of a dispute;
- Described an Automated Online Dispute Resolution (AODR) system which should be able to resolve all disputes cases automatically online. The existence of such a system should be able to help in lowering the cost of the dispute resolution process and the time taken to resolve any issue;
- Proposed a system for Quality certification for each soft-product which would have great benefit to the soft-products market and facilitate the use of new technologies in searching and acquiring such products;
- Studied some of the obstacles that currently preventing Saudi Arabia of benefiting from the e-commerce explosion, since it was identified as one of several countries with immense growth potential in the near future.

10.3 Future Research

The problem of resolving disputes regarding soft-products is complicated and difficult in terms of resolution. The work that has been undertaken in thesis is only a start, and directions for future research are suggested as follows:

- The potential for implementing the FAVS and possible problems;
- Studying the possibility of standardizing the certificates (Quality, Order, and Delivery) in order to expedite it before proprietary implementation is written.
- Trying to minimize the involvement of the TTPs in the ETP and study more the level of trust in every one.
- Looking in to the new contract languages like BCL [94] and the possibility if using it in writing the contract to expedite the contract processing and also to use the current standards.
- Studying the possibility of incorporating the TTP servers into the contract so the system can contact these servers directly without going back to the users.
- Automating the generation of the plug-ins by running the payment method through the taxonomy is something worth more investigation and study. (currently the dispute Plug-in is generated manually).
- Looking into having the AODR support new and more product types and payment methods.
- Study the possibility of given every payment method some properties which according to, evidence required can be specified. Therefore, if a new payment method is established, it should possible to run this method on a list of questions and come up with the required evidences to solve such disputes.
- Some research is being started looking into the possibility of qualifying services [98], and this still needs more look in to standardization.

Finally, the problem of dispute resolution is a major one. Whilst it should be considered from several different perspectives, sight should not be lost of the need for practicality in any solution being proposed. Research into this whole area will continue; this thesis should stand as a thorough piece of reference work for any subsequent activity in this field.

Bibliography

1. 123Callingcards, www.123callingcards.com, 10-10 2003.
2. ISO 7498-2, Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security architecture. International Organization for Standardisation, 1989.
3. ISO/IEC 9797, Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. ISO/IEC, April 1994 (second edition).
4. ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms. ISO/IEC, December 1994.
5. ISO/IEC 10181-1, Information technology - Open systems interconnection - Security frame works for open systems - Part 1: Overview. ISO/IEC, 1996.
6. ISO/IEC DIS 10181-4, Information technology - Open systems interconnection - Security frame works in open systems - Part 4: Non-repudiation. ISO/IEC, March 1995.
7. ISO/IEC 11770-2, Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques. ISO/IEC, 1996.
8. ISO/IEC 3rd CD 13888-1, Information technology - Security techniques - Non-repudiation - Part1: General model. ISO/IEC JTC1/SC27 N1274, March 1996.
9. ISO/IEC WD TR 14516-1, Guidelines for the use and management of trusted third parties - Part 1: General overview. ISO/IEC JTC1/SC27 N1235, November 1995.
10. ISO/IEC WD TR 14516-2, Guidelines for the use and management of trusted third parties - Part 2: Technical aspects. ISO/IEC JTC1/SC27 N1237, November 1995.
11. American Bar Association, Addressing Disputes in Electronic Commerce, 2004, law.washington.edu/ABAeADR/documentation/docs/FinalReport102802.pdf.
12. ABA Task Force on Electronic Commerce and ADR, Addressing Disputes in Electronic Commerce: Recommendations and report draft March 2002.
13. F. Al-Hoymany, E-Business and PKI in Saudi Arabia, 2002, <http://www.idsc.gov.eg/Conferences/SeminarE-business/E-business-in-Saudi.Pdf>.
14. Hartman et al, Net ready - Strategies for Success in the E-conomy, McGraw-Hill, New York, 2000.

15. Turban et al, Electronic Commerce 2002: A Managerial Perspective. New Jersey: Pearson Education, 2002.
16. Saleh Alfuraih, et al. Using trusted Email to Prevent Credit Card Frauds in Multimedia Products. World Wide Web 5(2): 245-262 (2002).
17. Saleh Alfuraih, et al. Trusted Email: A Proposed Approach to Prevent Credit Card Fraud in Softproducts E-Commerce. ICEIS (4) 2004: 106-113.
18. Saleh Alfuraih, R. Snow. Can Soft-Products Have Precise Quality as Hard Products, The IASTED International Conference on Web Technologies, Applications, And Services –WTAS- 2005.
19. Saleh Alfuraih, R. Snow. Taxonomy of E-commerce Disputes, WSEAS Transactions On Computers, Issue 6, Volume 3, December 2004.
20. Saleh Alfuraih, R. Snow. Soft-Products Fraud Prevention Using Trusted Delivery, WSEAS TRANSACTIONS on BUSINESS and ECONOMICS Issue 2, Volume 2, April 2005.
21. Saleh Alfuraih, R. Snow. ODR and the E-commerce, The IASTED International Conference on Web Technologies, Applications, And Services - WTAS- 2005.
22. Saleh Alfuraih, R. Snow. Location of Trusted Email for Prevention of Credit Card Fraud in Soft-Products E-Commerce, WSEAS Transactions On Computers, Issue 6, Volume 3, December 2004.
23. All-business, Why Accepting Credit Cards Can Boost Your Sales, 4-2 2005, <http://www.allbusiness.com/articles/EBusiness/911-2804-2814.html>.
24. AME-info.com, E-Commerce reaches new highs in Saudi Arabia, 2005, <http://www.ameinfo.com/61990.html>.
25. Antifraud.com, Online Fraud Prevention Tips, <http://www.antifraud.com/tips.htm>, 2004.
26. The Chartered Institute of Arbitrators, <http://www.arbitrators.org/>, 2005.
27. N. Asokan, V. Shoup, and M. Waidner. Optimistic fair exchange of digital signatures. In K. Nyberg, editor, EUROCRYPT '98, Lecture Notes in Computer Science, pages 591–606. Springer-Verlag, 1998. A longer version is available as Technical Report RZ 2973 (#93019), IBM Research, November 1997 at <http://www.zurich.ibm.com/Technology/Security/publications/1997/ASW97b.ps.gz>.
28. N. Asokan, M. Schunter, and M. Waidner. Optimistic protocols for fair exchange. In T. Matsumoto, editor, 4th ACM Conference on Computer and Communications Security, pages 8–17, Zurich, Switzerland, Apr. 1997. ACM Press.
29. N. Asokan, V. Shoup, and M. Waidner. Asynchronous protocols for optimistic fair exchange. in Proceedings of the IEEE Symposium on Research in Security and Privacy, May 1998. P. 86–99.

30. Auerbach, S. Jerold. (1983) Justice Without Law? Oxford: Oxford University Press.
31. Authorizenet.com, Security Best Practices - Protecting Your Business, 6-6 2004, <http://www.authorizenet.com/files/securitybestpractices.pdf>.
32. A. Bahreman, J. D. Tygar. Certified electronic mail, in: Symposium on Network and Distributed Systems Security, Internet Society, 1994, pp. 3–19.
33. Baldwin, Robert W., Chang V., "Locking the e-safe", IEEE Spectrum, p. 40 (1997).
34. The European Central Bank, ECB Blue Book 2002, 10-10 2004, www.ecb.int.
35. Bank_of_America, Dispute Guide Commercial Card Services, 07-01 2004, <http://www.purchasing.fsu.edu/pdf/DisputeGuide2001.pdf>.
36. F. Bao, R. H. Deng, W. Mao. Efficient and practical fair exchange protocols with off-line TTP, in: IEEE Symposium on Security and Privacy, 1998.
37. M. Ben-Or, O. Goldreich, S. Micali, R. Rivest, A fair protocol for signing contracts, IEEE Transaction on Information Theory 36 (1) (1990) 40–46.
38. Robert A. Bennett, CYBER FRAUD 'I DIDN'T DO IT', 1-2 2004, http://www.creditcollectionsworld.com/news/121401_3.htm.
39. BIS, Payment systems in Saudi Arabia 2003, <http://www.bis.org/publ/cpss59.pdf>.
40. C. Boyd, E. Foo. Off-line fair payment protocols using convertible signatures, Lecture Notes in Computer Science 1514 (1998) 271–285.
41. Maria Bruno, Microsoft Gives Boost to Surrogate Card Numbers. Bank Technology News <http://www.banktechnews.com/btn/articles/btnoct01-1.shtml>.
42. Card4Call, www.card4call.com, 10-10 2003.
43. Cartio, www.cartio.com, 10-8 2004.
44. Chaum, D., "Online Cash Checks", Proceedings of Eurocrypt 89, pp. 288-293 (1990).
45. Eric K. Clemons, M. C. Row. FT Survey on Mastering Management, "Behavior is Key to Web Retailing Strategy", Financial Times, Nov. 13, 2000.
46. ClicknSettle, <http://www.clicknsettle.com>.
47. ClickShare, www.clickshare.com, 10-8 2004.
48. T. Coffey, P. Saidha. Non-repudiation with mandatory proof of receipt, ACM CCR: Computer Communication Review 26.
49. Consumers-International, Disputes in Cyberspace, Survey, December 2000; pp. 23 and 24.

50. U.S.-Saudi Arabian Business Council, The Telecommunications and Information Technology Sectors in the Kingdom of Saudi Arabia, June 2005, <http://www.us-saudi-business.org/Telecom%20Report%20June%202005.pdf>.
51. B. Cox, J. D. Tygar, M. Sirbu, NetBill security and transaction protocol, in: USENIX Association (Ed.), Proceedings of the first USENIX Workshop of Electronic Commerce, USENIX, 1995, pp. 77–88.
52. S. Curry, An Inside Look at E-Commerce Fraud Prevention and Solutions, 06-13 2004, <http://www.scambusters.org/ecommercefraud.pdf>.
53. Cybersettle, <http://www.Cybersettle.com>.
54. R. H. Deng, L. Gong, A. A. Lazar, W. Wang, . Practical protocols for certified electronic mail, Journal of Network and System Management 4 (3) (1996) 279–297.
55. D.E. Denning, Protecting public keys and signature keys. IEEE Computer Magazine, 16(2):27-35, 1983.
56. Global Business Dialogue, Alternative Dispute Resolution Guidelines - Agreement reached between Consumers International and the Global Business Dialogue on Electronic Commerce <http://www.gbde.org/agreements/adragreement03.pdf>.
57. Direct.gov.uk, Money, tax and benefits, 15-12 2004, <http://www.direct.gov.uk>.
58. eBay, www.ebay.com.
59. Encyclopedia, encyclopedia.com, 9-8 2004.
60. European-Union, Recommendation 98/257/EC, Recommendation 2001/310/EC. <http://europa.eu.int>.
61. Mandana Jahanian Farsi, Digital Cash. Master Thesis, 1997 Department of mathematics and computing science Göteborg University.
62. Julie Ferguson, Five Tools You Can Use to Prevent Fraud, 8-7 2004, http://retailindustry.about.com/library/uc/02/uc_fraud1.htm.
63. Flohr, Udo, "Electric Money", Byte, p. 74 (1996).
64. Alan O. Freier, Philip Karlton, Paul C. Kocher. The SSL Protocol Version 3.0, Internet Draft Network Working Group, March 1996, <http://wp.netscape.com/eng/ssl3/ssl-toc.html>.
65. Lon. Fuller, The Forms and Limits of Adjudication, Harvard Law Review, 1978, vol. 92.
66. M. Galanter, "Reading the Landscape of Disputes: What We Know and Don't Know (and Think We Know) About Our Allegedly Contentious and Litigious Society." University of California Los Angeles Law Review 31(1983): 4-71.
67. Gemmell, Peter S., "Traceable e-cash". IEEE Spectrum. p. 35 (1997).

68. S. Ghosh, D.L. Reilly. Credit card fraud detection with a neural-network. System Sciences, 1994. Vol.III: Information Systems: Decision Support and Knowledge-Based Systems, Proceedings of the Twenty-Seventh Hawaii International Conference on Information Systems: Decision Support and Knowledge-Based Systems, 1994 Vol.III Page(s):621 –630.
69. Joseph Gibbons, Private Law, Public Justice: Another Look at Privacy, Arbitration and Global E-commerce, 15 Ohio State Journal On Dispute Resolution, 769-793 (2000).
70. S. Haber, W. S. Stornetta. How to time-stamp a digital document. Journal of Cryptology, 3(2):99-111, 1991.
71. Y. Han, Investigation of non-repudiation protocols, in: ACISP: Information Security and Privacy: Australasian Conference, Vol. 1172 of Lecture Notes in Computer Science, Springer-Verlag, 1996, pp. 38–47.
72. P.J.M. Havinga, G.J.M. Smit, A. Helme. "Survey of electronic payment methods and systems", Proceedings Euromedia 96, Society for Computer Simulation ISBN 1-56555-102-8, pp. 180-187, London, December 1996.
73. Veijo Heiskanen, Dispute Resolution in International Electronic Commerce, 16 Journal of International Arbitration 29-44 (1999).
74. Christopher T. Heun, Fear Of Fraud Informationweek.com March 4, 2002, <http://www.informationweek.com/story/IWK20020301S0002>.
75. J. Hornle, Online Dispute Resolution in Business to Consumer E-commerce Transactions, The Journal of Information, Law and Technology (JILT) 2002 (2) <http://elj.warwick.ac.uk/jilt/02-2/hornle.html>.
76. Julia Hörnle, Online Dispute Resolution in Business to Consumer E-commerce Transactions. Journal of Information, Law and Technology 2002(2): (2002).
77. VeriSign Inc., Digital Certificates, <http://www.verisign.com>.
78. ISO, ISO/IEC WD 138883. 6th working draft on Non-repudiation, Part 3: Mechanisms using asymmetric techniques. ISO/IEC JTC1/SC27 N993, 1995-04-07.
79. Kassedjian, Cahterine, Cahn, Sandrine,. Dispute Resolution Online, 32 Int'l Lawyer 977, 1998.
80. Ethan Katsh, Janet Rifkin, Alan Gaitenby. E-Commerce, E-Disputes, and E-Dispute Resolution: Learning from eBay and Other Online Communities," Ohio State Journal of Dispute Resolution (Summer 2000).
81. Ethan Katsh, Online Dispute Resolution: The Next Phase, Lex Electronica, Vol. 7. No. 2, Spring 2002 <http://www.lexelectronica.org/articles/v7-2/katsh.htm>.

82. Jörg Kienzle, Digital Money A divine gift or Satan's malicious tool? April 22, 1996.
83. S. Kremer, O. Markowitch. Optimistic non-repudiable information exchange, in: J. Biemond (Ed.), 21st Symp. on Information Theory in the Benelux, Werkgemeenschap Informatie- en Communicatietheorie, Enschede (NL), Wassenaar (NL), 2000, pp. 139–146.
84. Audri and Jim Lanford, Online Auction Fraud, 06-15 2004, http://www.marconeworld.com/issues/v3_i5/comp.htm.
85. United Nations Commission on International Trade Law, <http://www.uncitral.org>.
86. Madar-Research, <http://www.madarresearch.com>.
87. O. Markowitch, Roggeman, Y. Probabilistic non-repudiation without trusted third party, in: Second Conference on Security in Communication Networks'99, Amalfi, Italy, 1999.
88. O. Markowitch, S. Saeednia. Optimistic fair-exchange with transparent signature recovery, in: 5th International Conference, Financial Cryptography 2001, Lecture Notes in Computer Science, Springer-Verlag, 2001.
89. Olivier Markowitch, Steve Kremer. An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party. ISC 2001: 363-378.
90. J. L. Massey, Contemporary cryptology: an introduction. Contemporary cryptology-- The science of information integrity, G. J. Simmons ed., pp 1-39. IEEE Press, 1992.
91. Jon W. Matonis, Digital cash and monetary freedom. <http://www.nttam.com>, May 1995.
92. Glenn J. McLoughlin, Electronic Commerce: An Introduction, 10-11 2004, fpc.state.gov/documents/organization/12056.pdf.
93. S. Micali, Certified E-mail with invisible post offices, Available from author; an invited presentation at the RSA '97 conference (1997).
94. Guido Governatori and Zoran Milosevic, An Approach for Validating BCL Contract Specifications In Claudio Bartolini, Guido Governatori, and Zoran Milosevic (eds). Proceedings on the 2nd EDOC Workshop on Contract Architectures and Languages (CoALa 2005). Enschede, NL, 20 Septemebr 2005. IEEE Press.
95. C. J. Mitchell, F. Piper and P. Wild. Digital signatures. Contemporary cryptology - The science of information integrity, G. J. Simmons ed., pp 32-378. IEEE Press, 1992.
96. J. Mitsianis, A new approach to enforcing non-repudiation of receipt, manuscript (2001).
97. Mobile2meter, www.mobile2meter.com, 10-8 2004.

98. C. Molina-Jimenez, Shrivastava, S., Crowcroft, J. and Gevros, P. On the Monitoring of Contractual Service Level Agreements, In Proceedings of the IEEE Conference on Electronic Commerce CEC04, The First IEEE International Workshop on Electronic Contracting (WEC), San Diego, 6-9, 2004 .
99. Nordea, www.nordea.fi, 1-3 2005.
100. Internet Corporation For Assigned Names and Numbers, <http://www.icann.org/>, 2004.
101. ODR.info, Online Dispute Resolution, 2004, [http://www.odr.info/Introduction Encyclopedia.doc](http://www.odr.info/Introduction%20Encyclopedia.doc).
102. OECD, RESOLVING E-COMMERCE DISPUTES ON LINE, <http://www.oecd.org/dataoecd/5/42/31919880.pdf>, 2 2005.
103. Tatsuaki Okamoto, Provably secure and practical identification schemes and corresponding signature schemes. In Ernest F. Brickell, editor, Advances in Cryptology—CRYPTO '92, volume 740 of Lecture Notes in Computer Science, pages 31–53. Springer-Verlag, 1993, 16–20 August 1992.
104. Chan P.K., Fan W., Prodromidis A.L., Stolfo S.J. Distributed data mining in credit card fraud detection. IEEE Intelligent Systems Volume: 14 Issue: 6 , Nov.-Dec. 1999 Page(s): 67 -74.
105. PayPal, Fraud Protection Tips for Sellers, <http://www.paypal.com/cgi-bin/webscr?cmd=fraud-tips-sellers-outside>, 2004.
106. PayPal, <http://www.paypal.com>.
107. H. H. Perritt, Dispute Resolution in Cyberspace: Demand for New Forms of ADR, 15 Ohio State Journal of Dispute Resolution, 2000.
108. Portalify, www.portalify.fi, 11-3 2005.
109. D. Post, Engineering a Virtual Magistrate System. NCAIR Conference on Online Dispute Resolution, Washington, DC. May, 1996.
110. Saudi Post, www.sp.gov.sa.
111. G. Poupard, J. Stern. Security analysis of a practical “on the fly” authentication and signature generation, in: Advances in Cryptology: Proceedings of Eurocrypt'98, Vol. 1403 of Lecture Notes in Computer Science, Springer-Verlag, 1998, pp. 422–436.
112. Brause R., Langsdorf T., Hepp M. Neural data mining for credit card fraud detection. Tools with Artificial Intelligence, 1999. Proceedings. 11th IEEE International Conference on, 1999 Page(s): 103 -106.
113. M. O. Rabin, Transaction protection by beacons, Journal of Computer and System Sciences 27 (2) (1983) 256–267.
114. Rabo-Bank, www.rabobank.nl, 2-3 2005.

115. Mindwave Research, 6th Annual ONLINE FRAUD REPORT - Online Payment Fraud Trends and Merchants' Response, 2-6 2005, http://www.cybersource.com/resources/collateral/Resource_Center/whitepapers_and_reports/CYBS_2005_Fraud_Report.pdf.
116. Electronic Consumer Dispute Resolution, <http://www.ecodir.org>.
117. R. Rivest, The MD5 Message-Digest Algorithm, 2004, <http://www.faqs.org/rfcs/rfc1321.html>.
118. R. L. Rivest, A. Shamir, D. A. Wagner. Time-lock puzzles and timed-release crypto, Technical Report MIT/LCS/TR-684, Massachusetts Institute of Technology (Feb. 1996).
119. Rule, Colin. ODR for Business: B2B Ecommerce, Consumer, Employment, Insurance, and other Commercial Conflicts, New York, Jossey-Bass, 2002.
120. B. Schneier, Applied cryptography - Protocols, algorithms, and source code in C. New York: John Wiley & Sons, 1996 (second edition).
121. BankCard Services, FAQ1, 8-8 2004, <http://www.e-bankcard.com/faq1.htm>.
122. Sirbu, Marvin A, "Credits and Debits on the Internet", IEEE Spectrum. p. 23 (1997).
123. Skipjack, AVS/CVV2 Response Codes, 7-8 2003, https://vpos.skipjack.com/avs_cvv2_response_codes.htm.
124. Sky_Bank, Top 10 Common CHARGEBACK Reasons/Tips, 07-19 2004, <http://www.skyfi.com/aboutsky/chargeback.pdf>.
125. SmartSettle, <http://www.smartsettle.com>.
126. SquareTrade, <http://www.squaretrade.com/>.
127. Switch, <http://www.switch.co.uk>, 9-8 2004.
128. P. Syverson, Weakly secret bit commitment: Applications to lotteries and fair exchange, in: Proceedings of the 1998 IEEE Computer Security Foundations Workshop (CSFW11), 1998.
129. MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, INFORMATION AND TELECOMMUNICATION TECHNOLOGY In SAUDI ARABIA 11-11 2004, http://www.itu.int/dms_pub/itu-s/md/03/wsispc3/c/S03-WSISPC3-C-0025!!MSW-E.doc.
130. T. Tedrick, How to exchange half a bit, in: D. Chaum (Ed.), Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, New York and London, 1984, 1983, pp. 147-151.
131. T. Tedrick, Fair exchange of secrets, in: G. R. Blakley, D. C. Chaum (Eds.), Advances in Cryptology: Proceedings of Crypto 84, Vol. 196 of Lecture Notes in Computer Science, Springer-Verlag, 1985, pp. 434-438.
132. Tele-Fact, www.telefact.fr, 1-3 2005.

133. Thiessen, Ernest. Beyond Win-Win in Cyberspace, 15 Ohio State Journal of Dispute Resolution 2000.
134. TrustE, <http://www.TrustE.com>.
135. G. Tsudik, Message authentication with one-way hash functions. Computer Communication Review, 22(5):29-38, October1992.
136. UBid, www.ubid.com.
137. Inc Vantage Card Services, Prevent Chargebacks, <http://www.vantagecard.com/html/preventchargebacks.html>, 10-8 2004.
138. VISA-Europe, www.visaeu.com, 8-2 2005.
139. VISA, Verified by Visa, OCT 20 2003, https://usa.visa.com/personal/secure_with_visa/verified_by_visa.html
140. W.Diffie, M.E.Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (6) (1976) 644–654.
141. Mohamed S. Wahab, E-Commerce and Internet Auction Fraud: The E-Bay Community Model, 06/2004, <http://www.crime-research.org/articles/Wahab1>.
142. N. Zhang, Q. Shi. Achieving non-repudiation of receipt. The Computer Journal, 39(10):844-853, 1996.
143. J. Zhou, D. Gollmann. An efficient non-repudiation protocol. In PCSFW: Proceedings of The 10th Computer Security Foundations Workshop. IEEE Computer Society Press, 1997.
144. J. Zhou, R. Deng, F. Bao. Evolution of fair non-repudiation with TTP, in: ACISP: Information Security and Privacy: Australasian Conference, Vol. 1587of Lecture Notes in Computer Science, Springer-Verlag, 1999, pp. 258–269.
145. J. Zhou, D.Gollmann. Evidence and non-repudiation. Journal of Network and Computer Applications, London Academic Press, 1997.
146. Jianying Zhou, Dieter Gollmann. A fair non-repudiation protocol. In Proceedings of the IEEE Symposium on Research in Security and Privacy [IEEE96], p 55-61.