2020

Electronic Payments: Guide on Legal and Regulatory Reforms and Best Practices for Developing Countries

Benjamin Geva

Osgoode Hall Law School of York University, bgeva@osgoode.yorku.ca

Source Publication:

International Trade Centre

Electronic Payments

Guide on Legal and Regulatory Reforms and Best Practices for Developing Countries

International Trade Centre

TRADE IMPACT FOR GOOD

Electronic Payments:

Guide of Legal, Regulatory Reforms and Best Practices for Developing Countries

Benjamin Geva

Publisher: International Trade Centre

Title: Electronic Payments: Guide of Legal, Regulatory Reforms and Best Practices for Developing Countries

Publication date and place: Geneva, April 2020

Page count: [70]

Language(s): English

ITC Document Number: [Provided by CE]

Citation Geva, B., (2020). *Electronic Payments: Guide on Legal and Regulatory Reforms and Best Practices for Developing Countries*. International Trade Centre, Geneva, Switzerland.

For more information, contact: Professor Benjamin Geva, bgeva@osgoode.yorku.ca

About the paper

Electronic payments (e-payments) occur whenever payment instructions, initiated by a device such as a computer or mobile phone, enter a payments system via the Internet or any other telecommunications network. E-payments can be assisted by non-banking channels. They enhance the speed, efficiency and safety of payments. However, to reap all such benefits, e-payments require new legal and regulatory solutions to accommodate both the promise and risks inherent in the quickening pace of development. This Guide sets out a general framework addressing e-payment systems in a broad international/cross-border context, as well as addresses regulatory principles, risk of legal uncertainty and e-payments services under international trade law.

Acknowledgements

Benjamin Geva, Professor of Law, Osgoode Hall Law School of York University, Toronto, Canada, is the author of this paper. LL.B. (cum laude) (1970), Heb. U. Jerusalem; LL.M. and S.J.D Harvard Law School; Member of the Ontario Bar; specializing in banking, negotiable instruments, funds transfers, digital currencies, and payment and settlement systems. Professor of Law, Osgoode Hall Law School of York University, Toronto, Canada (faculty member since 1977); Counsel, payments and cards group in Torys LLP, Toronto (since 2012); founding Editor of the Banking and Finance Law Review; and author of Financing Consumer Sales and Product Defences, The Law of Electronic Funds Transfers, Bank Collections and Payment Transactions: Comparative Study of Legal Aspects, and The Payment Order of Antiquity and the Middle Ages: A Legal History.

Under the IMF technical assistance program, he advised and drafted key financial sector legislation, particularly payment laws, in several developing and post-conflict countries (particularly in the former Yugoslavia, Sri Lanka and Cambodia). In 2019, he participated, as ITC's legal expert on e-payments, in a National Public-Private Dialogue on E-Commerce Reforms in Sri Lanka organized under the EU-Sri Lanka Trade Related Assistance project.

Writer of numerous articles, particularly on funds transfers and negotiable instruments; held numerous visiting positions in United States universities (Chicago, Illinois, Northwestern, Duke program in Hong Kong, and Utah), Australia (Melbourne, Monash, Deakin and Sydney), Israel (Tel Aviv), Singapore (National University of Singapore), as well as in France (Aix en Province) and Germany (Hamburg); also held research fellowships at Oxford, Cambridge, Max-Planck Institute for Comparative and Private International Law (Hamburg) and New York University; member of MOCOMILA (Monetary Committee of the International Lawyers' Association) and working groups drafting domestic and international legislation on personal property security, securities transfers, letters of credit, and payment systems. He is now observer in the Joint Study Committee on the Uniform Commercial Code (UCC) and Emerging Technologies in the United States.

Rajesh Aggarwal, Chief, Trade Facilitation and Policy for Business (TFPB), International Trade Centre (ITC), initiated the project and provided substantive guidance.

Giles Chappell, Trade Policy Advisor, TFPB, ITC, provided logistical support; Ana Correia, Vidya Nathaniel and Devika Rajeev, TFPB, ITC, and Simona Ristic, Osgoode Hall Law School (2021 Graduating Class) provided review and editorial support.

Contents

Figures

Acronyms

AISP	Account Information Service Provider
Art./Arts.	Article/Articles
ASEAN	Association of Southeast Asian Nations
ASPSP	Account Servicing Payment Service Provider
ATM	Automated Teller Machine
B2B	Business to Business
B2P	Business to Person
BI	Bank Indonesia
BIS	Bank for International Settlements
CC	Credit Card
CPMI	Committee on Markets and Infrastructures
CPSS	Committee on Payment and Settlement Systems.
DNS	Deferred net settlement
EPS	Electronic Payment Services
EU	European Union
FI	Financial Institution
GATS	General Agreement on Trade in Services
GGNPSD	General Guidance for National Payment System Development
IRT	International Remittance Transfer
KYC	Know your customer
MLICT	Model Law for International Credit Transfers
P2B	Person to Business
P2P	Person to Person
PIS	Payment Initiation Service
PISP	Payment Initiation Service Provider
POS	Point of Sale
PSD	Payment Services Directive
PSD2	Second Payment Services Directive
PSP	Payment Service Provider
RSP	Remittance Service Provider
RTGS	Real-time gross settlement
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TPP	Third-party processor
UCC	Uniform Commercial Code
UNCITRAL	United Nations Commission on International Trade Law
US	United States of America
USMCA	Agreement between the United States of America, the United Mexican States and Canada
WTO	World Trade Organization

Executive summary

E-payments occur whenever payment instructions, initiated by a device such as a computer or mobile phone, enter a payments system via the Internet or any other telecommunications network. E-payments enhance the speed, efficiency and safety of payments. Specifically, the support provided by e-payments to e-commerce has facilitated retail commerce between remote parties, with non-cash payments that can be assisted by non-banking channels. However, to reap all such benefits, e-payments require new legal and regulatory solutions to accommodate both the promise and risks inherent in the quickening pace of development.

Participants in the e-payments landscape are customers, direct clearers, indirect clearers, and money transmitters (also known as payment institutions). Customers are payers and payees, usually buyers and sellers of goods or services, respectively. The other players are payment service providers. Of those, direct clearers are typically large, regulated financial institutions (usually banks), each having a direct relationship with the central bank. Indirect clearers are typically small, regulated financial institutions, each with a correspondent relationship with a direct clearer. Money transmitters are payment service providers that are not regulated as financial institutions, each having a relationship with either direct or indirect clearers. Other participants may be various intermediaries acting on behalf of all such players in interacting with others – for example, processors.

E-payments help overcome complicated and costly processes related to physically collecting cash payments for a product sold online. This is particularly important for cross-border e-commerce. At the same time, regulatory gaps make it difficult for e-payment models to take off in developing counties.

In addressing best practices and regulatory and legal reforms, this Guide outlines the issues and discusses proposed solutions under selected models from both developed and developing countries. Chapter 1 addresses the principal transactions: card payments, e-money transfers, fast/faster payments, and remittances. It then sets out a general framework that addresses e-payment systems in a broad international/cross-border context. Chapter 2 addresses regulatory principles underlying e-payments and trade policy. Chapter 3 addresses the risk of legal uncertainty. Chapter 4 discusses e-payments services under international trade law. An extensive Appendix presents the treatment of the legal risks under Art. 4A of the American Uniform Commercial Code (UCC) and the European Union (EU) Second Payment Services Directive (PSD2).

A competitive environment requires interoperability and elimination of entry barriers both domestically and internationally. A common framework consisting of the following regulatory principles, agreed upon by several nations, could help underline any applicable services market access commitments made:

- Sound legal and regulatory frameworks.
- Balanced oversight and supervision.
- Technology-neutral regulatory approaches.
- Encouraging innovation.
- Wide access to the payment system.
- Risk-based policies and regulations.

The elimination of legal uncertainty in the smooth operation of the payment system has been a stated goal of policymakers. A comprehensive, and yet specific, payment law thus ought to be multifaceted. An underlying assumption is the existence of a sound legal system containing solid laws, addressing subjects such as contract, property, credit, secured credit, and insolvency, as well as sound and reliable mechanisms for the administration of justice and dispute resolution. Furthermore, an assumption is to be made as to the existence of effective financial regulation addressing central banking, financial institutions, and markets. The final assumption to be made is the existence of clear currency laws establishing an official currency, providing for legal tender, and possibly regulating the use of foreign currency. With all of this is taken to be in existence,

the focus of the present discussion is on specific laws addressing non-cash payments – namely those payments that are not exclusively made in cash. The emphasis is on institutions and transactions.

Thematically, payment law may be divided as follows:

- Payment system law governing the regulation and oversight of core interbank clearing and settlement systems;
- Payment transactions law governing rights and remedies of all participants from end-to-end in carrying out a payment transaction; and
- Payment services law governing (i) the regulation and oversight of providers of payment services which are not regulated financial institutions, as well as (ii) rights and remedies of end-participants of a payment transaction, namely, the payer and payee, vis-à-vis the payment service provider with which the end-participant is in privity. The latter aspect overlaps with a portion of payment transactions law. However, it is not limited to the rights and remedies of end-participants towards their payment service providers and also addresses rights and remedies of, and towards, intermediaries in the payment transactions. At the same time, in contrast to payment transactions law, which covers only the payment transaction itself, payment services law covers the broader contractual relationship between end-parties and their respective payment service providers, within which payment transactions are carried out.

Pragmatically, however, it may be preferable to address payment law as consisting of the following more or less distinct components:

- The organization and operation of clearing and settlement systems, particularly those which are the main engine of the national payment system;
- The identification of policy objectives and/or the policy-setting body for payment systems in general, particularly the national systems;
- Risk to economic and financial activity incurred in connection with carrying out payment transactions;
- The licensing or regulation of payment service providers which are not regulated financial institutions, particularly unregulated deposit takers; and
- Rights and remedies of participants in a non-cash payment transaction.

Topics to be addressed by payment transactions legislation cover payment orders, third-party processors, completion of credit transfer and discharge, completion of the debit transfer and discharge, mistaken or fraudulent payments: liability, damages and restitution, and accounts. Specific issues to be addressed are:

- Scope;
- The payment order and its acceptance or rejection;
- Timely cancellation and automatic withdrawal of an (unexecuted) payment order;
- Sender’s payment obligation and its excuse under “money-back guarantee” upon non-completion of a credit transfer;
- Sender’s payment;
- Sender’s liability;
- Fraudulent and mistaken (albeit authorized) payment orders;
- Finality of payment: completion of credit transfer and discharge of underlying debt;
- Liability for losses by a Receiving Bank;

- Restitution upon erroneous completion of credit transfers;
- Third-party Intermediaries;
- Law applicable: variations and cross-border- international setting.

Cross-border payment services may be governed by the General Agreement on Trade in Services (GATS) and regional free trade agreements.

CHAPTER 1 WHAT IS AN E-PAYMENT?

Introduction

Historically, payment instructions accessing bank money were made orally or, more typically, in the form of writing. Use of telecommunication, first the telegraph and then the transatlantic cable, goes back to mid-19th century.[1] For its part, the roots of electronic banking can be traced to the automated processing of paper instruments such as cheques occurring in the mid-20th century.[2] However, the watershed of electronic banking, where payments are processed as well as transmitted electronically so as become *electronic payments* (*E-payments)*, is a development of the second part of the 20th century. Once it became possible to transmit instructions from a computer or computer terminal, the electronic funds' transfer was born. Telecommunication in the electronic age was originally on cable or wire;[3] subsequently, the wireless option became available,[4] and ultimately, instructions could be transmitted over the Internet.[5]

E-payments occur whenever payment instructions, initiated by a device such as a computer or mobile phone, enter a payments system via the Internet or any other telecommunications network.[6] More specifically as to their emergence and evolution,[7]

> In mid-20th century, breakthroughs in mainframe computing enabled inter-bank settlement, which gave rise to open-loop payment cards. In the 1960s and 1970s, magnetic stripe technology brought the digitization of the point of sale. By the late 1990s, electronic commerce had become mainstream, creating new opportunities for Internet payments. The advent of smartphones and connected devices in the 2010s gave rise to mobile and omni-channel commerce, blurring the boundaries between in-store and online shopping. To keep pace, online marketplaces, bricks and mortar retailers, participants in the sharing economy, and government agencies are all demanding new ways to pay and be paid. Payment technology companies are extending network capabilities to support the long tail of innovation. The retail payments industry is characterized by specialization and collaboration, with many companies working together to deliver a secure and reliable service.

E-payments enhance the speed, efficiency and safety of payments. Specifically, the support provided by e-payments to e-commerce has facilitated retail commerce between remote parties, with non-cash payments that can be assisted by non-banking channels. This has brought significant benefits for both merchants of goods and services and their buyers. For merchants, e-payments facilitate the collection of payments, thereby making e-commerce possible and practical in the first place. In solving the collection difficulty and enabling merchants to reach remote places and unbanked buyers, e-commerce, supported by e-payments, facilitates easier access to a much wider buyer-base throughout a region or country, as well as across the

---

[1] See Douglas W Arner, Janos N Barberis & Ross B Buckley, "The Evolution of Fintech: A New Post-Crisis Paradigm?" at 4, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676553>, accessed 24 January 2020.

[2] See in general e.g. Benjamin Geva, "Is Death of the Paper Cheque Upon Us? The Electronic Presentment and Deposit of Cheques in Canada" (2014) 30 BFLR 113; Benjamin Geva, "From Paper to Electronic Order: The Digitalization of the Check in the USA" (2015) 4 JLIA 96.

[3] For an early discussion on the subject see Israel Sendrovic, "Technology and the Payment System" in Bruce J Summers, ed, The Payment System: Design, Management and Supervision (Washington: International Monetary Fund, 1994) at 178.

[4] See Gianni Bonaiuti, "Economic Issues on M-Payments and Bitcoin" in Gabriella Gimigliano, ed, Bitcoin and Mobile Payments Constructing a European Union Framework (London: Palgrave, 2016) at 27.

[5] See CPSS, "Innovations in retail payments" (Basel: BIS, May 2012), online: <https://www.bis.org/cpmi/publ/d102.pdf>, accessed 24 January 2020. See also: CPSS, "Survey of developments in electronic money and internet and mobile payments" (Basel: BIS, March 2004), online: <https://www.bis.org/cpmi/publ/d62.pdf>, accessed 24 January 2020.

[6] Payment Systems Worldwide, "Developing a Comprehensive National Retail Payments Strategy Consultative Report" (The World Bank, July 2012) at 105, online: <http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1323805522895/Developing_a_comprehensive_national_retail_payments_strategy_consultative_report(8-8).pdf>, accessed 24 January 2020 [hereafter, "National Retail Payments Strategy"].

[7] World Economic Forum, "Addressing E-Payment Challenges in Global E-Commerce" (White Paper, May 2018) at 3, online: <http://www3.weforum.org/docs/WEF_Addressing_E-Payment_Challenges_in_Global_E-Commerce_clean.pdf>, accessed 24 January 2020.

globe. The other side of the same coin is that e-payments have provided buyers with greater convenience and choice in the form of access to a broader range of suppliers and products.

All such benefits are substantial for both merchants and customers in developing countries, where a sizeable portion of the population is unbanked and has no easy access to physical retail outlets. This is true domestically as well as for cross-border e-commerce, enhanced by e-payments infrastructure, which can help developed countries become more competitive and diversify their exports. Having evolved to become the norm in developed countries, e-payments are essential for the growth, integration and competitiveness of developing countries in the global economy that has increasingly become both borderless and digitized.

To reap all such benefits, however, e-payments require new legal and regulatory solutions to accommodate both the promise and risks inherent in the quickening pace of development.

The evolving e-payments landscape introduces both new players and new payment methods. Thus, other than regulated banks or other financial institutions, some of which hold accounts with the central bank and some of which do not (direct clearers and indirect clearers, respectively), new players include 'money transmitters', also called payment institutions. The new methods are effectively enhanced old methods that have enhanced operability and yet increased risk.

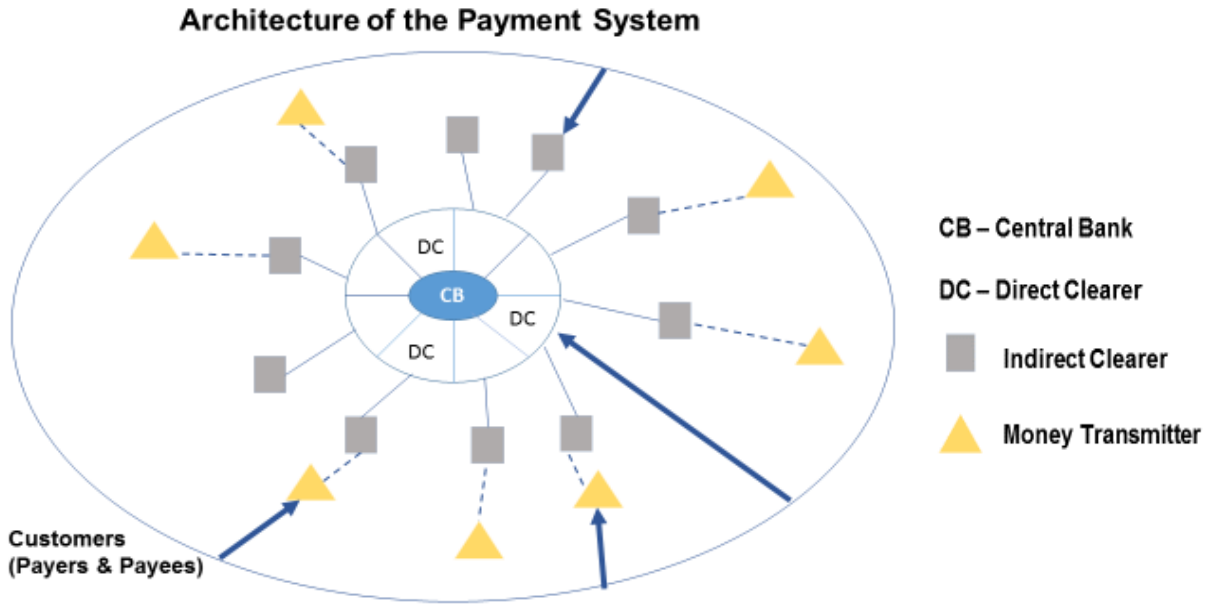
More specifically, participants in the e-payments landscape are customers, direct clearers, indirect clearers, and money transmitters (also known as payment institutions). Customers are payers and payees, usually buyers and sellers of goods or services, respectively. The other players are payment service providers. Of those, direct clearers are typically large regulated financial institutions, usually banks, each having a direct relationship with the central bank. Indirect clearers are typically small, regulated financial institutions, each with a correspondent relationship with a direct clearer. Money transmitters are payment service providers that are not regulated as financial institutions, each having a relationship with either direct or indirect clearers. Other participants may be various intermediaries acting on behalf of all such players in interacting with others, for example, processors. They are not included in the ensuing Figure 1.

The following Figure 1 depicts graphically the architecture of a national payment system comprising of:

- Customers having direct relationships with money transmitters, indirect clearers, or direct clearers;
- Indirect clearers standing in privity with direct clearers;
- Money transmitters having direct relationships with either indirect clearers or direct clearers;
- Only direct clearers have a direct relationship with the central bank;
- Customers – whether payees or payers, businesses or consumers –located on the outside circle.

One could add to the illustration networks of money transmitters, each having an account with a bank – which is the case in a mobile network.

Figure 1 The architecture of the payment system



Depending on their nature, electronic payments may be processed in either a high (or large) value or retail network. Payments processed in retail networks are typically high-volume, relatively low-value transactions consisting of cash withdrawals at Automated Teller Machines (ATMs), payments to third parties, and transfers from one account to another belonging to the same person. Payments to third parties may be either non-cash from end to end – whether face to face or between remote parties – or either commenced and/or concluded in a cash payment – as is typical in the case of remittances. E-payments may be single, immediate standing orders (preauthorized) or 'post-dated' and are typically settled on a deferred net settlement (DNS) basis. Payments may be person to business (P2B), business to person (B2P), business to business (B2B) or person to person (P2P).

E-payments help overcome complicated and costly processes related to physically collecting cash payments for a product sold online. This is particularly important for cross-border e-commerce. At the same time, regulatory gaps make it difficult for e-payment models to take off in developing counties. To begin with, there may be restrictions on the establishment of non-bank payment providers, coupled with disproportional know your customer (KYC) regulation, lack of interoperability with the financial system, stringent reserve and currency requirements, regulations that create local monopolies, and skewed playing field for participants. For example, a large number of countries have regulatory frameworks in place discouraging or complicating the emergence of mobile money services. Additionally, many countries do not provide adequate protection to users of e-payment services. In some places, all of this is the result of monopolies and successful lobbying of interest groups. Elsewhere it may be simply an issue of calibration of financial laws to accommodate the emergence of new players and modified payment methods.

This Guide is designed to provide a blueprint for best practices and regulatory and legal reforms covering e-payments for developing countries. It recognizes that much has already been achieved in such countries,[8]

[8] See in general for developing countries: John Effah, "Institutional Effects on E-payment Entrepreneurship in a Developing Country: Enablers and Constraints" (2016) 22:2 Information Technology for Development 205, online: <https://www.tandfonline.com/doi/full/10.1080/02681102.2013.859115>, accessed 26 February 2020; for INDIA: Hemlata Chelawat & IV Trivedi, "Implications of Emerging Electronic Payment Systems in India: A Strategic Overview" (2014) 6:3 J Multidiscip Res 53, online: <http://www.jmrpublication.org/portals/jmr/Issues/JMR6-3.pdf>, accessed 26 February 2020; Saroj Kumar Singh, "E-Payment – A Study of Banking System in India" (2016) 3:6 AEBM 646, online: <https://www.krishisanskriti.org/vol_image/15Dec201606124217%20%20%20%20%20%20%20Saroj%20Kumar%20Singh%20%20%20%20%20%20%20%20%20646-649.pdf>, accessed 26 February 2020; Sreeja Mohan & Dr TR Anil Kumar, "Cash Less India: An Overview To The Digital Revolution In The Indian Banking Sector" (2020) 68:43 Our Heritage 569, online: <https://archives.ourheritagejournal.com/index.php/oh/article/view/4685>, accessed 26 February 2020;

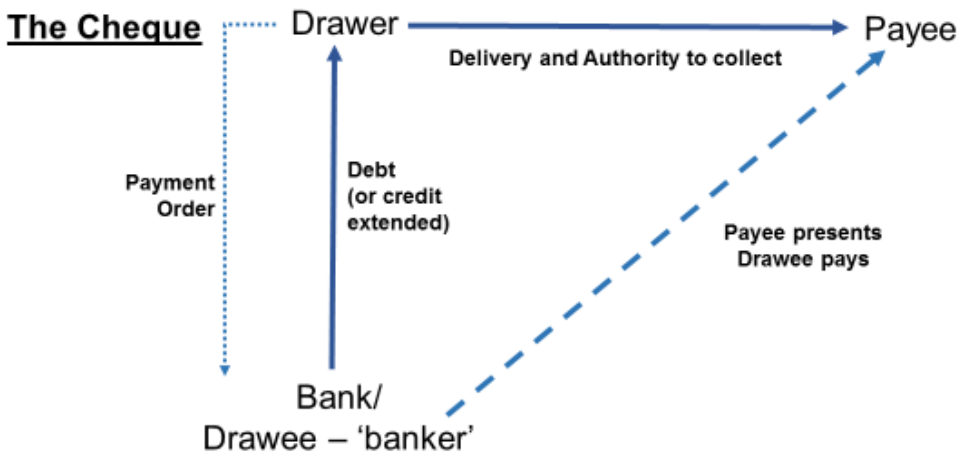
but is not designed such as to give an encyclopaedic review of all such relevant developments. Rather, this Guide outlines principal issues and presents selected models for their resolution from developed and developing countries. The Guide proceeds as follows: this chapter sets out the prevalent e-payment methods, namely, card payments, e-money transfers, fast/faster payments, and remittances. The chapter then sets out a general framework addressing e-payment systems in a broad international/cross-border context. Chapter 2 addresses regulatory principles underlying e-payments and trade policy. Chapter 3 addresses the risk of legal uncertainty. Chapter 4 discusses e-payments services under international trade law. An extensive Appendix presents the treatment of the legal risk under Art. 4A of the American Uniform Commercial Code (UCC) and the European Union (EU) Second Payment Services Directive (PSD2).

Card payments

At their inception, card payments were paper-based. In comparison to the personal cheque, the added advantage to the payee of the card payment is the benefit from the issuer's obligation, typically the payer's bank.

Thus, in Figures 2-3 that follow, the drawer is the payer, issuing a cheque to the payee, drawn on the drawee bank acting for the drawer-payer as a paymaster (PM). Whether the drawee bank is obligated to pay the payee is a matter under the banking agreement, exclusively between the drawee bank and its customer, i.e. the drawer, so that even where there is such an obligation, it is not part of the cheque transaction and is unenforceable by the payee. The dishonour of the cheque is at the payee's risk, whose recourse in such a case is solely against the drawer.

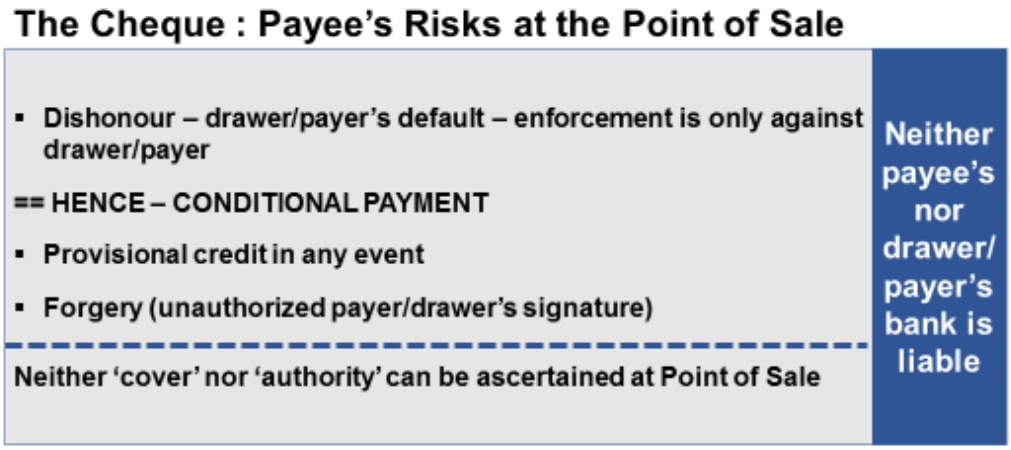
Figure 2 The Cheque



Drawer instructs **Drawee** to pay and by issuing cheque to **Payee** authorizes **Payee** to collect from **Drawee** by presenting the cheque to **Drawee**.

The Reserve Bank of India, "Payment and Settlement Systems in India: Vision – 2019-2021" (2019), online: <https://rbidocs.rbi.org.in/rdocs/PublicationReport/PDFs/PAYMENT1C3B80387C0F4B30A56665DD08783324.PDF>, accessed 26 February 2020; for **MALAYSIA**: Evelyn Peiqi Ooi Widjaja, "Non-Cash Payment Options in Malaysia" (2016) 33:3 JSEAE 398, online: <https://www.jstor.org/stable/44132413>, accessed 26 February 2020; and for **THAILAND**: Tarra Theisen, "Beating the Legislation Lag: the Dynamic Development of Thailand's E-Commerce Industry" (2018) International Immersion Program Working Paper No 73, online: <https://chicagounbound.uchicago.edu/international_immersion_program_papers/73>, accessed 26 February 2020.

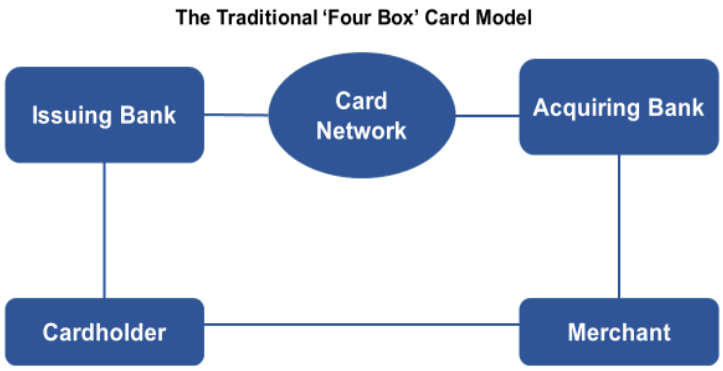
Figure 3 The cheque: payee's risks at point of sale (POS)



At the same time, unlike a payee of a cheque, a payee in a card transaction does not have to be concerned whether payment will be refused since payment is confirmed by the issuer. Card payments are carried out from either the payer's credit line or the payer's asset (or current) account. In the former case, we speak of a credit card and in the latter of a debit card. At present, card payments are predominantly electronic, i.e. the payer's instruction is electronic and not on a signed paper, even where the latter is required for evidentiary purposes.

An electronic card transaction typically commences by inserting the card into a merchant's terminal and authenticating the instruction by entering a secret code – a Personal Identification Number (PIN). A card transaction may, however, be initiated without the physical card, by passing on card information in writing, by telephone, or from a computer terminal or digital device such as a smartphone, possibly over the internet, or via a website. Either way, even if the transaction is initiated by inserting the card and signing a sales draft, based on which funds are transferred and settled, information is passed on exclusively electronically. For a full electronic initiation, several countries recently embraced the EMV (Europay, MasterCard, Visa) standard. This is an open-standard set of specifications for smart card payments and acceptance devices premised on chip technology for a card, which provides enhanced security and fraud protection. The EMV standard also accommodates near-field communication (NFC) communication, enabling contactless PIN-less as well as PIN access.

Figure 4 Traditional 'Four Box' card model



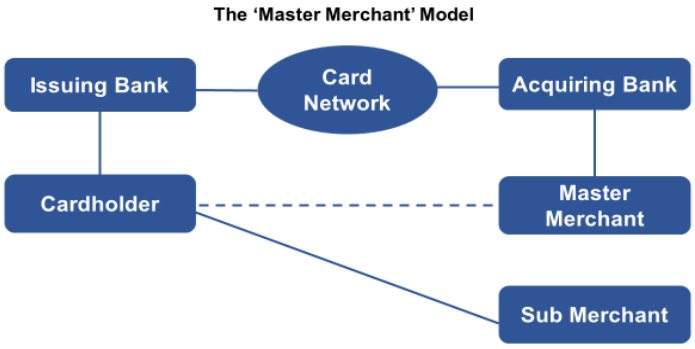
Participants in a typical inter-bank[9] payment card transaction, as set out in Figure 4, are a cardholder, a merchant, an issuing bank, and an acquirer (the merchant's bank). The issuer incurs a payment obligation, which benefits the payee-merchant at least indirectly. The issuer and acquirer are member banks in a card network association, which establishes rules and standards governing the issuance and use of the cards. Usually, a member bank both issues cards and acquires merchants who will accept the cards. In a given transaction, a member bank may thus act as either an issuer or acquirer (or both, in which case the transaction is not 'inter-bank'). Currently, two

[9] Participants need not necessarily be 'banks' but could be other financial institutions. They are nevertheless predominantly 'banks' and, in any event, the term 'bank' is loosely used here to denote any financial institution participating in a credit card scheme.

for-profit associations, Visa and MasterCard, with American Express trailing third, dominate the credit card landscape across the world. All three are global multi-currency international systems. Debit cards scheme tends to be domestic and of smaller scope. As outlined below in Chapter 1, 'e-money transfers', a card may also be loaded with e-money or be prepaid.

In a credit card scenario that originated in the e-commerce space, as set out in Figure 5, small merchants may act as 'sub-merchants' using a card network indirectly through a 'master merchant', such as PayPal or Square, acting on their behalf. The master merchant positions itself between such small merchants and the acquirer. More specifically, the master merchant acts in the transaction as the payee – dealing directly with both the acquirer and the cardholder/payer — and separately accounting to the sub-merchant.[10]

Figure 5 The 'Master Merchant' model



The contractual network that binds participants in a card payment is quite complex. Separate bilateral contracts exist between the processor and the card association, the issuer, and the acquirer, as well as between the card association and the issuer and the acquirer. They all require the issuer, acquirer and the processor to comply with the card association rules. Such rules govern the issuance and use of cards branded by the card association. As undertaken by them in their respective agreements with the card association, member banks and processors contractually require merchants to comply with identified parts, albeit not all, of the association rules. For its part, the processor in a card transaction is responsible for supplying POS terminals to merchants and is acting to connect them to member banks. As such, it is a party to processing contracts with merchants as well as with member banks. It is, however, not a party to each individual card payment transaction.

By way of summary, the card association has contracts with member banks. In a card payment transaction, each such bank acts as an issuer and/or an acquirer, as demonstrated in Figure 6. The card association also has a contract with the processor. The processor has its own contracts with merchants, the card association, and member banks. The acquirer is in a contractual relationship with the merchant, while the issuer is under a contract with the cardholder. Each pair of bank members does not have a specific contract but card association rules are likely to serve as a binding contract among all of them. The cardholder and merchant are parties to the transaction for the sale of goods or services for which payment is made. As well, the card association rules bind in their entirety the issuing and acquiring bank and the processor. They bind merchants only in part and do not bind directly the cardholder. Figure 6 and 7 below demonstrates the contractual relationships between the various parties engaged in a card payment transaction and the process followed to facilitate such a transaction.

[10] Carol Coye Benson & Scott Loftesness, "Interoperability in Electronic Payments: Lessons and Opportunities" (CGAP 2012) at 14-16, online: <https://www.cgap.org/sites/default/files/Interoperability_in_Electronic_Payments.pdf>, accessed 24 January 2020.

Figure 6 Credit card network[11]

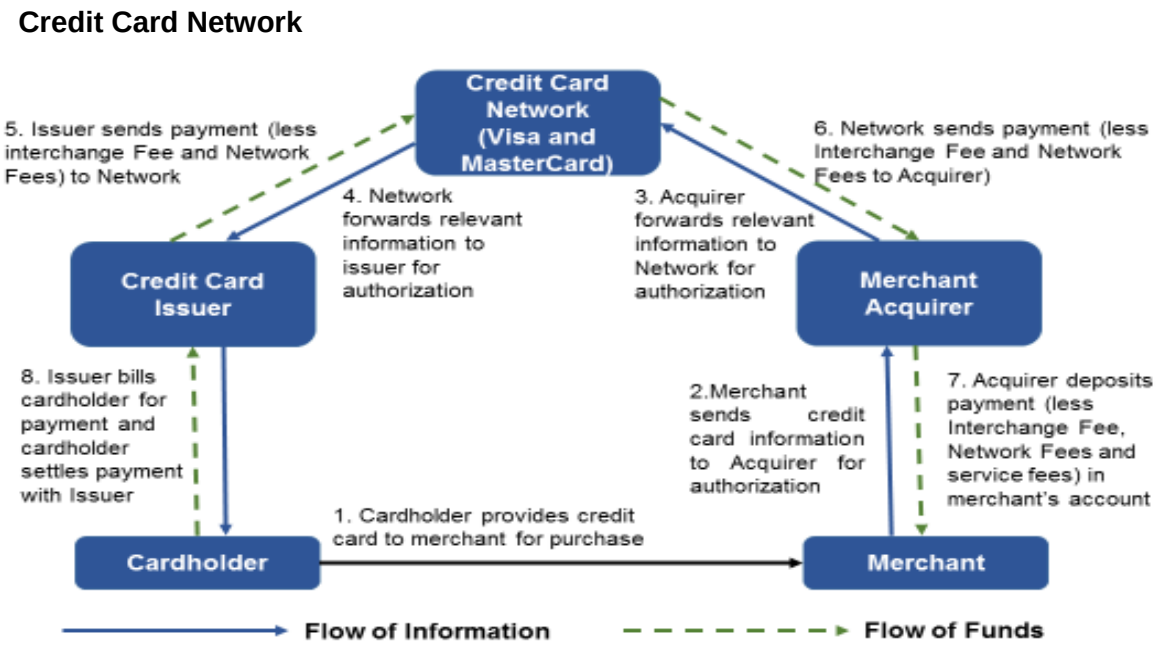
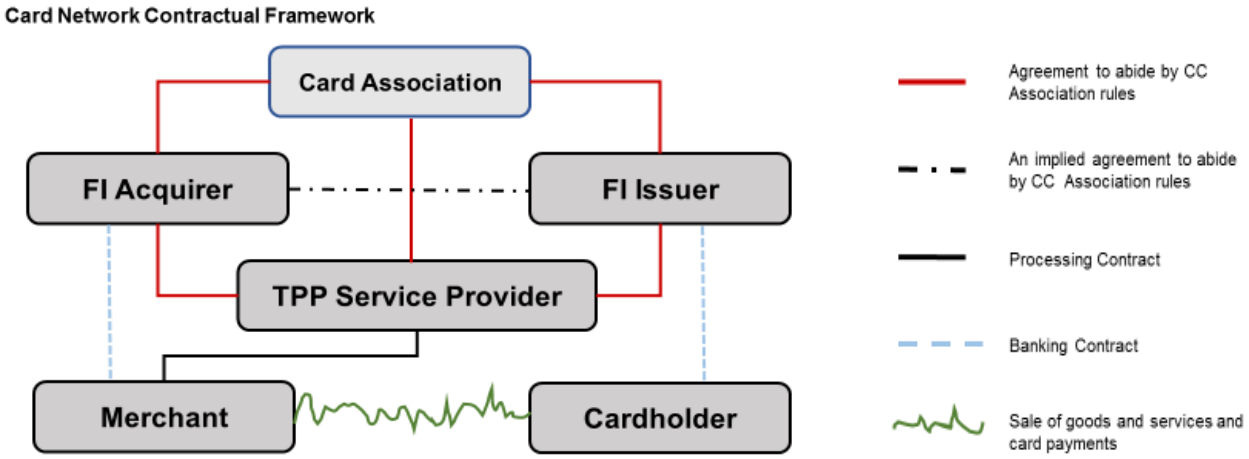


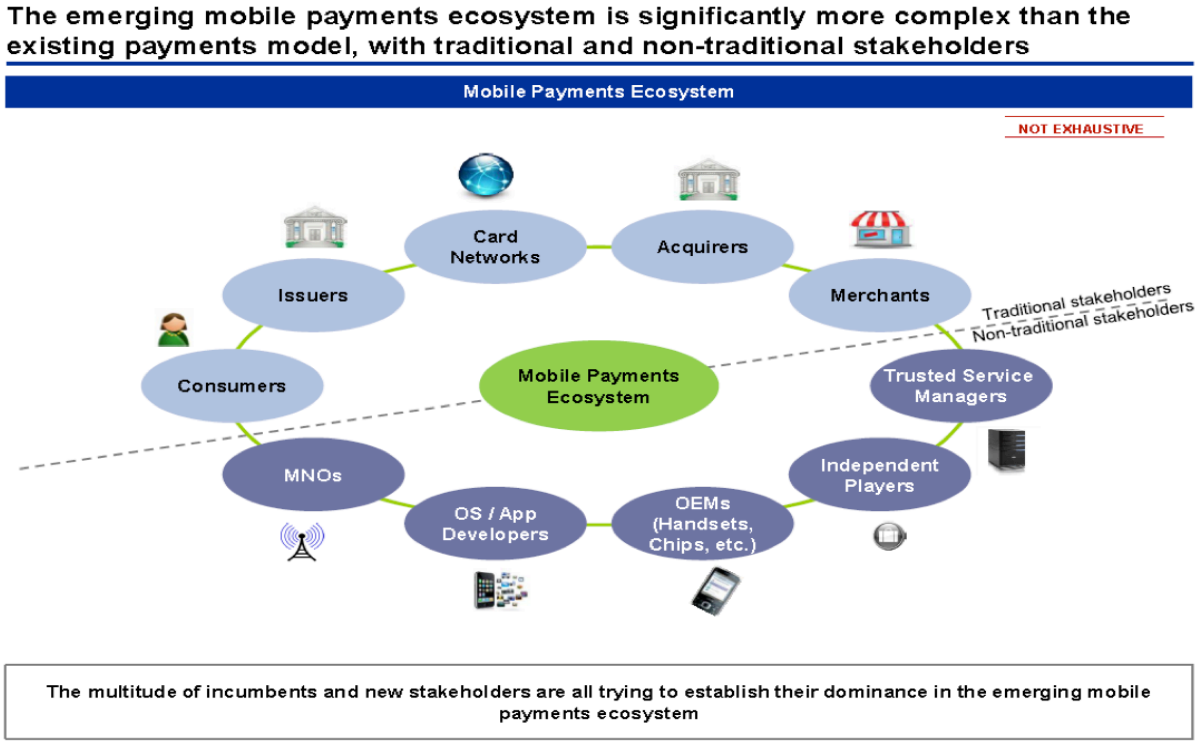
Figure 7 Card network contractual framework



It is possible to have one or more card credentials stored in an electronic wallet. Payment by card through mobile phones has generated a new multi-participant ecosystem that adds new participants to the card transaction, such as a Mobile Network Operator (MNO) and Trusted Service Manager (TSM), who do not participate in the payment transactions but facilitate its occurrence.

[11] The Commissioner of Competition v. Visa Canada Corporation and MasterCard International Incorporated et al. (8 May 2012), CT-2010-010 (Notice of Application of the Commissioner of Competition) at paragraph 39.

Figure 8 Mobile payment ecosystem[12]



Legal principles governing card payments may be tentatively summarized as follows:

- Card payment is typically initiated by the payer who, with the consent of the payee, inserts a card at a POS terminal, and seeks acceptance of the request, as provided in applicable contracts. The communication of such requests over the network constitutes the transmittal of the payment instruction.

- The payer's request may either be accepted or rejected by the issuer/payer's bank. It shall be accepted if made according to the contract between the payer and the issuer/payer's bank and there is adequate cover (including under any approved credit line) in the payer's account. Rejection or non-acceptance in breach of this provision charge the payer's bank with liability to the payer for the wrongful dishonour of the payer's payment instruction.[13] Non-acceptance caused either by system malfunction not attributed to the fault of any participating bank, or by system maintenance at reasonable intervals, will not constitute such a breach.

- Upon the payer's confirmation or approval of the amount of payment, the payment instruction becomes irrevocable and cannot be cancelled. The request for confirmation or approval sent by the issuer/payer's bank, the payer's confirmation or approval, and the acceptance or rejection by the issuer/payer's bank are to be advised per system rules and applicable contracts in immediate response to the payment instruction.

- Acceptance by the issuer/payer's bank of the payment instruction, when received by the payee, to the extent of its amount as accepted upon the payer's confirmation or approval:

[12] Source: Vipul Lalka, Deloitte.

[13] It is a question of policy then whether the scope of liability for such wrongful dishonour is to be restricted to a particular amount.

- Entitles the payee – at least towards the acquirer/payee's bank[14] – to unconditionally obtain credit to the payee's account;
- Binds the issuer/payer's bank to pay the acquirer/payee's bank;
- Binds the payer to pay the issuer/payer's bank and entitles the issuer/payer's bank to have the payer's account debited or otherwise obtain reimbursement from the payer; and
- Constitutes an absolute discharge of the debt paid by the payer to the payee.[15]

The time, manner, and charges for carrying out these obligations are governed by network rules and applicable bilateral contracts.

- In initiating payment over a network, the payer warrants to the payee and each participating bank that the card to be used is valid and that value to be applied in payment is genuine.[16]
- A person to whom a device was issued is responsible for any communication either over a network or per its governing rules or procedures, given by him or her, under his or her authority, or that has been authenticated under a commercially reasonable security procedure agreed upon between the issuer of the device and that person. This rule does not exclude a consumer protection type regulation setting a ceiling to customer's exposure.

The operation of a global interbank scheme is premised on the interoperability among various national schemes. Network interoperability thus allows customers of a bank in one system access to the infrastructure of another system. For example, a cardholder whose account is in Bank A in Country A may use the card in payment to a merchant in Country B whose account is with Bank B in Country B. Banks A and B are not members of the same network, but the customer of Bank A is given access to the infrastructure provided by Bank B to its customer. In general,

> an interoperable payments system enables the seamless participation of two or more proprietary acceptance and processing platforms, and possibly even of different payment products, thereby promoting competition and also enabling economies of scale.[17]

Accordingly, under a more comprehensive explanation, 'interoperability' is defined to mean:

> a situation in which payment instruments belonging to a given scheme may be used in other countries and in systems installed by other schemes. Interoperability requires technical compatibility between systems, but can only take effect where commercial agreements have been concluded between the schemes concerned.[18]

---

[14] It may be unnecessary to provide the payee with an additional right directly against the payer's bank. Adequate protection is given to the payee as the payee is provided with a right against the payee's bank, which in turn becomes entitled to recover from the payer's bank. It is thus the obligation of the payer's bank to pay the payee's bank, which constitutes "money" with which payment is made to the payee and with which the payer's obligation is discharged. Yet, the actual risk of default by the payer's bank does not fall on the payee, but rather, on the payee's bank. This may be necessary for the maintenance of the integrity of the system since the payee may not have had any dealing with the payer's bank and is likely to rely on the payee's bank.

[15] At least under Charge Card Services Ltd., [1988] 3 All ER 702 (CA).

[16] This warranty is analogous to an undertaking by a payer that banknotes and coins used in cash payment are genuine.

[17] The World Bank, "Financial Infrastructure Series Payment Systems Policy and Research, Innovation In Retail Payments Worldwide: A Snapshot" (October 2012) at 32, online: <http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1323805522895/Innovations_in_retail_payments_worldwide_consultative_report(10-17).pdf>, accessed 24 January 2020.

[18] Committee on Payment and Settlement Systems, "A glossary of terms used in payments and settlement systems" (Basel: BIS, March 2003) at 27, online: <https://www.bis.org/cpmi/glossary_030301.pdf>, accessed 24 January 2020. See also: Payment Systems Worldwide, "Developing a Comprehensive National Retail Payments Strategy: Consultative Report (2012) The World Bank at 105, online: <http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1323805522895/Developing_a_comprehensive_national_retail_payments_strategy_consultative_report(8-8).pdf>, accessed 2 March 2020.

E-money transfers

Developments exploiting technological achievements have not been limited to communication. It has also become possible to load monetary value (that is, value denominated in an official or any other unit of account) on a tamper-resistant stored-value device such as a card or personal computer. In such a case, the value becomes known as 'electronic money' or 'e-money'. The majority of e-money schemes have involved 'balance-based' products. In such products, devices store and manipulate a numeric ledger, with transactions performed as debits or credits to a balance. Accordingly, this type of e-money is a monetary balance or value recorded electronically on and is available from a stored-value product (SVP), such as a chips card, a hard drive in a personal computer, or a server.[19] Such a record, accessible from the device without resort to the bank's computer system, can be viewed as a decentralized bank account.[20] E-money is said to 'differ … from so-called access products, which are products that allow consumers to use electronic means of communication to access otherwise conventional payment services' in and out bank accounts.[21] Issuers of e-money need not necessarily be banks.

Under a variant of a balance-based e-money product, monetary value is not loaded on the device; rather, it is available from a master account, belonging to the issuer or someone acting on the issuer's behalf.[22] As in the case of e-money, monetary value is not available from the payer-debtor's own bank account.[23] However, such prepaid value is in a bank account, even if it is not that of the payer. Its use entails communication to the issuer and requires the cardholder to access a bank account (even if not their own). From this perspective, a prepaid product device is more a variant of an access device, rather than of a SVP.

A payment order issued from a digital device such as a mobile phone, rather than from a computer terminal or computer, is often said to result in a 'mobile payment'. When the payment scheme is operated over mobile devices, it is even described as involving 'mobile money'. However, in substance, a payment order initiated from a digital or mobile device is a species of electronic funds transfer.[24] For its part, mobile money is value loaded on – or made available from an issuer's master account through mobile devices - rather than retrieved by them from users' bank accounts. As such, it is a form of e-money. It is, therefore, confusing to treat such developments as reflecting a 'digitization of state-issue currenc[y]', even in connection with an on-line (e-commerce) transaction.[25]

E-money transfers are to be distinguished from peer-to-peer payments in digital coins. Much like an electronic payment instruction, a digital coin consists of encrypted data expressed in strings of bits. However, as 'an entity that amounts to a string of bits', a coin's string represents value and should have a unique identity.[26] Like physical coins and banknotes, digital coins are not paid out of bank accounts so that their payment does not appear to require intermediation by banks. Rather, as is the case for electronic funds transfers, digital coins are paid over the cyberspace. Peer-to-peer payments in digital coins are outside the scope of this Guide.

---

[19] CPSS and the Group of Computer Experts of the central banks of the Group of Ten countries, "Security of electronic money" (Basel: BIS, 1996) particularly at 5, online: <https://www.bis.org/cpmi/publ/d18.pdf>, accessed 24 January 2020. See also information on "electronic money" online: <https://en.wikipedia.org/wiki/Electronic_money>, accessed 24 January 2020.

[20] Alan L Tyree, "The Legal Nature of Electronic Money" (1999) 10 JBFLP 273 at 276.

[21] CPSS, "Implications for Central Banks of the Development of Electronic Money" (Basel, October 1996) at 1, emphasis in the original; online:<https://www.bis.org/publ/bisp01.pdf>, accessed 24 January 2020.

[22] For the view that this is in fact e-money in the true sense, see: Nadia F. Piffaretti, "A Theoretical Approach to Electronic Money" (1998) FSES-302. online SSRN: <https://ssrn.com/abstract=70793> or <http://dx.doi.org/10.2139/ssrn.70793>, both accessed 24 January 2020.

[23] Unfortunately, the confusion between these two types of payment products is rampant. For a definition of "e-money" that does not include the prepaid product, see Ben Fung, Miguel Molico and Gerald Stuber, "Electronic Money and Payments: Recent Developments and Issues" (2014) Bank of Canada Discussion Paper 2014-2, online: <http://www.bankofcanada.ca/wp-content/uploads/2014/04/dp2014-2.pdf>, accessed 24 January 2020.

[24] Whether from (or into) an asset account, credit line, or stored-value – as the case may be.

[25] Notwithstanding Joshua S. Gans & Hanna Halaburda, "Some Economics of Private Digital Currency" (2013) Bank of Canada, Working Paper 2013-38, online: <http://www.bankofcanada.ca/wp-content/uploads/2013/11/wp2013-38.pdf>, accessed 24 December 2020.

[26] Gideon Samid, Tethered Money: Managing Digital Currency Transactions (London: Academic Press, 2015) at 105-106.

Fast(er) payments

A relatively novel development is the emergence of Fast (or Faster) Payment Services (FPS). The FPS is a near real-time payment capability for credit transfers. It is an automated clearing system for electronic retail transfers, in which debit and credit entries are posted to the respective originator's and beneficiary's accounts with the processing of each payment order, albeit possibly operating as a deferred multilateral net settlement system. As such, even as it is not a real-time gross settlement (RTGS) system, FPS is a near Real-Time Credit System, typically providing immediate payment to the beneficiary;[27] it also facilitates the real-time transfer of data relating to the payment.[28]

An FPS makes funds immediately available to the payee and can be used around-the-clock, on a 24/7 basis. As such, it overcomes the limitations of traditional retail payment services, namely that the funds usually reach the beneficiary one or more days after the funds are debited in the payer's account, and that these can be initiated only in certain places at certain times.

As a specific type of retail payment, an FPS gives rise to risks in payment infrastructures and retail payment services.[29] The main risk categories are legal, credit, liquidity and operational risk. The latter include security risks, particularly caused by fraudulent activity. For its part, reputational risk depends on ethics, safety, security and quality of service, and may lead to increased operating, capital or regulatory costs. As for the legal risk,[30]

> Fast payments, like other retail payment services, need to be supported by sound legal arrangements according to their specific design, operation and use. The legal framework needs to clearly determine the applicability of laws and regulations in order to avoid losses or disruptions related to the lack of or unexpected application of the legal framework. The legal framework needs to establish, and provide legal protections around, when, inter alia, payments are final and when the funds are legally transferred from sender to receiver. This clarity is needed to allocate responsibilities between the payer and the payee vis-à-vis their respective PSPs and also to understand the respective responsibilities between PSPs, as well as between PSPs and the central clearing and settlement system. PSPs also need clarity on the rules and regulations that apply when they process fast payments. These rules could be general (i.e. not specific to fast payments), but the speed that characteristics fast payments could make it more challenging to fulfil some of the requirements. Legal frameworks should also provide a sound basis for protecting the netting and settlement arrangements.
>
> It is especially important in fast payments to design rules and procedures allowing post-transaction resolution of fraudulent or erroneous transactions. The related customer liability aspects must also be considered. Even though all these issues affect retail payments in general, clarity, awareness and legal certainty are especially important for fast payments, as they are new implementations.

[27] Where it is not an RTGS System, the FPS will usually provide immediate payment to the beneficiary on the basis of risk control measures such as sender cap, bilateral credit limits, collateralization and loss sharing.

[28] For the global trend in this direction see: Committee on Markets and Infrastructures (CPMI), "Fast payments—Enhancing the speed and availability of retail payments" (Basel: BIS, 2016), online:<http://www.bis.org/cpmi/publ/d154.pdf>, accessed 24 January 2020. The report sets out key characteristics of fast payments, takes stock of different initiatives in CPMI jurisdictions, analyzes supply and demand factors that may foster or hinder their development, sets out the benefits and risks and, finally, examines the potential implications for different stakeholders, particularly central banks.

[29] For an overview of key risks in financial market infrastructures including payment infrastructures see CPMI & Technical Committee of the IOSCO, "Principles for financial market infrastructures" (Basel: BIS, 2012), Chapter 2, online: <https://www.bis.org/cpmi/publ/d101a.pdf>, accessed 24 January 2020. Risks in retail payments have also been discussed in CPMI, "Clearing and settlement arrangements for retail payments in selected countries" (September 2000) at Chapter 4, online: <https://www.bis.org/cpmi/publ/d40.pdf>, accessed 24 January 2020. More recently, risks in retail services were reviewed in CPSS, "Innovations", supra n 5 and CPMI, "Non-banks in retail payments" (Basel: BIS, September 2014) at Chapter 4, online: <https://www.bis.org/cpmi/publ/d118.pdf>, accessed 24 January 2020.

[30] CPMI, "Fast Payments", *supra* n. 28, at 49.

Remittances

For their part, remittances can be either domestic or international, with the latter raising most issues.[31]

International Remittance Transfers (IRTs) are:

- Cross-border person-to-person payments of relatively low value
- In practice: recurrent payments by migrant workers
- Indistinguishable from other low-value cross-borders transfers
- Mostly credit transfers: payment initiated by the sender's instruction to the capturing Remittance Service Provider (RSP)

Elements of an IRT are:

- Capturing – sender's payment; identification of end parties; "location" – either physical or virtual
- Disbursement – usually in cash; identification of receiver
- Messaging – information may travel with the funds – but could travel independently
- Settlement
- Liquidity – e.g. when the disbursing agent pays before receiving funds

Sender's payment could be in cash, by card, or from a bank account.

IRT Participants are:

- End parties:
  - Sender-payer, originator
  - Receiver-Payee, beneficiary
- Remittance Service Providers (RSPs):
  - Capturing RSP
  - Disbursing RSP
- RSPs' Agents
- Banks

The network connecting the capturing and disbursing RSP may be unilateral, franchised, negotiated or open. Other than over unilateral networks, and particularly over open ones, IRTs require extensive use of transfers via intermediate or correspondent banks.

Electronic payment systems: regional initiatives

An e-payment is carried out over an electronic payment system. For its part, an electronic payment system requires one or more networks, each consisting of a collection of computers, servers, mainframes, network

[31] See in general, CPSS & World Bank, "General principles for international remittance services" (Basel: BIS, January 2007), online: <https://www.bis.org/cpmi/publ/d76.pdf>, accessed 24 January 2020.

devices, peripherals, or other devices connected to one another to allow the sharing of data.[32] An in-house bank network links only customers of that bank. Correspondent banking links two banks and their customers, and may link even more banks and their customers through multiple interbank bilateral relations. A multilateral interbank payment system links banks, and thus their networks and customers, into one scheme.

Interconnection means the technical ability to connect with another computer or network.[33] For example, the Internet, defined as an open worldwide communication infrastructure consisting of interconnected computer networks and allowing access to remote information and the exchange of information between computers,[34] facilitates such communication among various computers (and not only within a network).

Interconnection is a necessary but insufficient condition for carrying out payments. Thus, each payment requires banking relationships including originating and destination accounts.[35] An interbank arrangement also requires an interbank clearing and settlement facility. To enhance interbank payments from end to end across more than one network, short of network integration, network interoperability is required.

Integration means taking different things and making them the same – effectively merging them. So far as interconnection is concerned, integration means putting different things on the same path, speaking the same language. On the other hand, interoperable systems 'don't have to be similar, don't have to [be] "speaking the same language" – but they can still effectively hand off data and move things from one standpoint to another.'[36] Accordingly,

> Broadly speaking, an interoperable payments system enables the seamless participation of two or more proprietary acceptance and processing platforms, and possibly even of different payment products, thereby promoting competition and also enabling economies of scale.[37]

Under a more comprehensive explanation, 'interoperability' is:

> a situation in which payment instruments belonging to a given scheme may be used in other countries and in systems installed by other schemes. Interoperability requires technical compatibility between systems, but can only take effect where commercial agreements have been concluded between the schemes concerned.[38]

A seamless flow of e-payments will benefit from interconnection, interoperability or integration, particularly in an environment that fosters harmonization, if not uniformity, in regulation, standards, rules and laws. This

---

[32] For this definition of "network" see: Computer Hope, "Network" (13 November 2018), online (dictionary definition): <https://www.computerhope.com/jargon/n/network.htm>, accessed 2 March 2020.

[33] See e.g. World Bank, "Achieving interoperability in mobile financial services: Tanzania – case study" (2015) World Bank Group (Washington, DC) Working Paper No 128225 at 8, online: <http://documents.worldbank.org/curated/en/740981531310065590/pdf/WP-TZ-Mobile-interoperability-10-03-2015-PUBLIC.pdf>, accessed 2 March 2020. See also Mobile Financial Services Working Group (MFSWG), "Mobile Financial Services: Basic Terminology", Guideline Note, (2012) Alliance for Financial Inclusion at 7, online: <https://www.afi-global.org/sites/default/files/publications/MFSWG%20Guideline%20Note%20on%20Terminology.pdf>, accessed 2 March 2020.

[34] Committee on Payment and Settlement Systems, "A glossary of terms used in payments and settlement systems" (Basel: BIS, March 2003) at 27, online: <https://www.bis.org/cpmi/glossary_030301.pdf>, accessed 24 January 2020.

[35] For a single payment for a non-customer payer, the originating account may be an ad hoc one (or internal to the originating bank) and where payment to the payee is in cash, the destination account may be internal to the destination bank.

[36] PYMNTS, "Why the Future of Payments is Interoperable (Not Integrated)",(18 December 2017), online: PYMNTS <https://www.pymnts.com/news/digital-banking/2017/modo-payments-bruce-parker-interoperable-payment-methods/>, accessed 2 March 2020.

[37] Payment Systems Worldwide, "Innovation in Retail Payments Worldwide: A Snapshot"(2012) The World Bank: Financial Infrastructure Series Payment Systems Policy and Research at 32, online: <http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1323805522895/Innovations_in_retail_payments_worldwide_consultative_report(10-17).pdf >, accessed 2 March 2020.

[38] Committee on Payment and Settlement Systems, "A glossary of terms used in payments and settlement systems" (Basel: BIS, March 2003) at 27, online: <https://www.bis.org/cpmi/glossary_030301.pdf>, accessed 24 January 2020. See also: Payment Systems Worldwide, "Developing a Comprehensive National Retail Payments Strategy: Consultative Report (2012) The World Bank at 105, online: <http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1323805522895/Developing_a_comprehensive_national_retail_payments_strategy_consultative_report(8-8).pdf>, accessed 2 March 2020.

is particularly apparent in an international/cross-border setting in which each country has its own regulators, laws, and banking systems. To that end, the experience in Europe is illuminating.

Thus, in its proposal for a Directive on payment services in the internal market (the Proposal),[39] the Commission of the European Communities (Commission) purported to provide for 'a harmonized legal framework' designed to create 'a Single Payment Market where improved economies of scale and competition would help to reduce the cost of the payment system.' Being 'complemented by industry's initiative for a Single Euro Payment Area (SEPA) aimed at integrating national payment infrastructures and payment products for the euro-zone', the Proposal was designed to 'establish a common framework for the Community payments market creating the conditions for integration and rationalization of national payment systems.' Focusing on electronic payments, and designed to 'leave maximum room for self-regulation of industry,' the Proposal purported to 'only harmonizes what is necessary to overcome legal barriers to a Single Market, avoiding regulating issues which would go beyond this matter.'[40]

As ultimately adopted, the first Directive on payment services in the internal market - that is, the original 'Payment Services Directive' or PSD[41] – implemented this vision. Its scope, as stated in Art. 2(1), is to 'apply to payment services provided within the Community,' both nationally and cross-border.[42]

With the advent of Internet banking and other technological innovations in payments, the need arose to upgrade the PSD, primarily to accommodate an integrated European market for card, internet and mobile payments.[43] To that end, among others, the second Payment Services Directive was passed in 2015. Since then, it has been implemented in the various national legislations in the course of 2018 (hereafter, the 'Directive' or 'PSD2').[44]

A more modest regional e-payment initiative is now in the working in countries that are members of the Association of Southeast Asian Nations (ASEAN). Thus, in 2019, against 'a lack of standardized e-payments',[45] the ASEAN e-Payments Coalition identified four areas for cooperation between the public and

---

[39] Commission of the European Communities, "Implementing the Community Lisbon programme: Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 97/7/EC, 2000/12/EC, and 2002/65/EC {SEC(2005) 1535}" (Brussels: 1 December 2005), online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2005:0603:FIN>, accessed 2 March 2020. Quotations in the text are from the Explanatory Memorandum, under "Context of the Proposal," id, which further cites Arts. 47(2) and 95(1) of the EC Treaty as the legal basis for the proposal. The proposal was discussed by Benjamin Geva, "Recent International Developments in the Law of Negotiable Instruments and Payment and Settlement Systems" (2007) 42 Tex Intl LJ 685 at 712–725 For the original PSD, see e.g. Benjamin Geva, "The EU Payment Services Directive: An Outsider's View" (2009) 28 Yearbook of European Law 177, Oxford University Press (editors Eeckhout and Tridimas), and in a comparative context: Benjamin Geva, "The Harmonization of Payment Services Law in Europe and Uniform and Federal Funds Transfer Legislation in the USA: Which is a Better Model for Reform?" (2009) 4 EUREDIA (Revue Européenne de Droit Bancaire et Financier/European Banking and Financial Law Journal) 699.

[40] Explanatory Memorandum, id, under "Legal Elements of the Proposal."

[41] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC, and 2006/48/EC and repealing Directive 97/5/EC, (OJ L 319 of 5.12.2007, p. 1–36), online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007L0064>, accessed 2 March 2020.

[42] This is in departure from European Parliament and Council Directive 97/5/EC of 27 January 1997 on cross-border credit transfers [OJ L 43 of 14.02.1997], ("the Transparency Directive") that was superseded by Title III and repealed by the Payment Service Directive.

[43] As envisaged by European Commission's Green Paper, "Towards an integrated market for cards, internet, and mobile payments", Green Paper (Brussels: 1 November 2011) COM(2011) 941 final, online: <https://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-941-EN-F1-1.Pdf>, accessed 2 March 2020; followed by European Commission, "Feedback Statement on European Commission Green Paper: Towards an integrated European market for card, internet, and mobile payments" (undated), online: <http://frob.pl/wp-content/uploads/2012/04/EC-feedback_statement_green-paper-card-internet-mobile-June-2012.pdf>, accessed 2 March 2020; and European Parliament resolution of 20 November 2012 on "Towards an integrated European market for card, internet and mobile payments" (2012/2040(INI)), P7_TA(2012)0426, for which motion dated 4 October 2012 is online: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0304+0+DOC+XML+V0//EN>, accessed 2 March 2020.

[44] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366>, accessed 2 March 2020. See Benjamin Geva, "Payment Transactions under the EU-Second Payment Services Directive (PSD2) – An Outsider's View" (2019) 54 TILJ, 211.

[45] The Economist Intelligence Unit, "Case Study: Digital payments in ASEAN – going cashless" in "Digital Platforms and Services: A development opportunity for ASEAN" (2019) The Economist at 14, online: <https://www.slideshare.net/economistintelligenceunit/digital-platforms-and-services-a-development-opportunity-for-asean>, accessed 27 February, 2020.

private sectors with the view to improving payments in the region: speed and convenience, regional standardization and interoperability, financial literacy and inclusion, and trust and security.[46]

For its part, the ASEAN Economic Community Blueprint 2025 identified financial integration, inclusion, and stability as components of a highly integrated and cohesive economy so as to be a characteristic and elemental aspect of the blueprint. In this context, with the view 'to foster stability and efficiency within as well as outside the region.' two goals were specifically highlighted. First, the enhancement of payment and settlement systems 'in several areas such as promoting standardization and developing settlement infrastructure for cross-border trade, remittance, retail payment systems and capital market.' Second, the endeavor to achieve 'a certain level of harmonization of standards and market practices based on international best practices…'[47] Digital integration is also identified as a priority area to '[e]nable seamless digital payments.'[48] Finally, 'the importance of safe and secure, efficient, and interoperable e-payment systems; is recognized in Art. 9 of the ASEAN Agreement on Electronic Commerce.[49]

Progress in the area is apparent.[50] However, as the EU experience demonstrates, to facilitate a seamless e-payment flow in a region, there is also a need to enhance at least harmonization, if not uniformity, in the legal and regulatory framework. Certainly, ASEAN, like most world regions, lacks both the domination of a single currency and the degree of political and institutional integration of the EU. Hence, political action must make up for those disadvantages in order to achieve an optimal degree of harmonization, if not uniformity, in regulation and laws.

The blueprint put forward by this Guide is designed to satisfy the needs of both national and regional/super-national frameworks.

Concluding Observations

In its strict sense, an e-payment transaction is paper-less, from end to end. It could be made in, but is not limited to, an e-commerce or online transaction. For their part, e-payments enhancing speed and efficiency are essential components of e-commerce, and require comprehensive, interoperable, national and cross-border banking and legal arrangements. Retail e-payments consist of cash withdrawals, transfers from one account to another belonging to the same person, and non-cash payments to third parties, such as remittances, P2B, B2P, B2B, and P2P. An e-payment can be carried out from, as well as into, an account with a bank or another payment service provider, a pre-paid product, or in digital coins. At the same time, a payment transaction may be carried out electronically only in part – and a discussion on the legal framework covering e-payments ought to take this into account.

E-payment laws cover:

- E-commerce (e-transactions) law infrastructure;
- The regulation and licensing of Payment Service Providers (PSPs) – insofar as they are not already regulated financial institutions;

---

[46] Digital ASEAN Initiative, "ASEAN e-Payments Coalition: e-Payment Recommendation Paper" (2019) World Economic Forum Working Paper, online: <https://weforum.ent.box.com/v/epaymentsrecommendationpaper>, accessed 2 March 2020.

[47] ASEAN Secretariat Jakarta, "ASEAN Economic Community Blueprint 2025" (2015) at 7-10 (quote is from A.4. (18(ii) at 10), online: <https://asean.org/?static_post=asean-economic-community-blueprint-2025>, accessed 2 March 2020.

[48] ASEAN, "ASEAN Digital Integration Framework" (undated), online: <https://asean.org/storage/2019/01/ASEAN-Digital-Integration-Framework.pdf>, accessed 27 February, 2020.

[49] ASEAN Agreement on E-commerce (2019), online: <https://eccil.org/euro-lao-business/asean-and-aec/asean-agreement-on-e-commerce-2/>, accessed 2 March 2020.

[50] See e.g. SWIFT, "Achieving Financial Integration in the ASEAN Region"(24 March 2017) SWIFT Discussion Paper, online: <https://www.swift.com/news-events/news/achieving-financial-integration-in-the-asean-region>, accessed 27 February, 2020. See also: the ASEAN Post Team, "E-Wallets could boost the region's tourism industry" (18 March 2018) the ASEAN Post, online: <https://theaseanpost.com/article/e-wallets-could-boost-regions-tourism-industry>, accessed 27 February, 2020; Morgan Stanley, "Disruption Decoded: Who Will Winn in ASEAN e-Payments" (undated) online: <https://www.morganstanley.com/ideas/asean-epayments>, accessed 27 February, 2020.

- Payment Systems – including clearing and settlement;
- Positions of participants other than payers, payees, and payment service providers, such as TPP (third-party-processors) vs. payment initiation service providers (PISPs) and account information service providers (AISPs); and
- Payment transactions governed by bilateral and multilateral contracts, statutes, regulations, and rules.

For their part, e-payments in retail transactions are predominantly credit transfers. More on such transfers and the law governing them is in the Appendix.

CHAPTER 2 E-PAYMENTS AND TRADE POLICY: UNDERLYING REGULATORY PRINCIPLES

A competitive environment requires interoperability and elimination of entry barriers both domestically and internationally. A common framework consisting of the following regulatory principles agreed among several nations could help to underline any applicable services market access commitments made:[51]

- **Sound legal and regulatory frameworks:** e-payment regulatory frameworks should provide clear definitions of the roles and responsibilities of the various parties involved in the payment system, including which laws and regulations apply to each of these, and how any relevant supervisory authority may conduct appropriate oversight. Overall financial regulatory frameworks should also look to implement e-payment-related rules in a coherent manner. In some instances, particularly around e-payment service innovations, different regulatory authorities may require specific information or impose specific processes, but may not be collaborating with each other, leading to further fragmentation.

- **Balanced oversight and supervision:** oversight and supervision of payment systems are crucial for maintaining their integrity and stability. One of the main objectives of oversight and supervision is the reduction of systemic risk, which could result from legal, liquidity, credit, operational, settlement and/or reputational risk in the payment system. To the greatest extent possible, oversight should proceed on a collaborative basis with industry to ensure policy and regulations reflect actual operating conditions and the overall business environment. Oversight should also take into account the possibility that unnecessarily broad regulations could have unintended consequences that may inhibit investment and innovation in e-payment systems.

- **Technology-neutral regulatory approaches:** as far as possible, regulatory frameworks should be neutral with regard to the payment technology and should focus on the functions of the service being offered. A functional approach allows banks and non-bank PSPs to compete in the different market segments and establish various partnerships for the supply of e-payment services. The ability of frameworks to stay up to date with technological developments to ensure balanced outcomes is also important.

- **Encouraging innovation:** in the face of technological change, it has become an increasingly common practice to enable innovation by creating regulatory safe zones. These “regulatory sandboxes” are controlled environments in which certain requirements are temporarily suspended or additional support measures are provided to allow experimentation with new products, most likely with a limited number of consumers. The approach enables technology firms and financial institutions to collaborate in a less regulated, closed marketplace, with the end result being more effective technology that benefits both businesses and consumers. It also enables regulators to better understand the benefits and impacts of a potential technology or payment method being applied more widely.

- **Wide access to the payment system:** the regulatory framework should be flexible enough to accommodate innovative payment services and to allow increased access by new participants, such as non-bank PSPs, and other niche service suppliers. Policy-makers may also want to think about the degree to which licensing requirements for the provision of e-payment services are transparent, objective and accessible – including by suppliers not based within the territory.

- **Risk-based policies and regulations:** policies and regulations dealing with issues such as KYC, anti-money laundering/combating the financing of terrorism (AML/CFT), preventing fraud and cybercrime, currency and reserve requirements, and data protection should all be applied in a way that is commensurate with associated risk – regardless of who is supplying that service. For example,

[51] E-payment regulatory principles as they appear verbatim in World Economic Forum, “Addressing E-Payment Challenges in Global E-Commerce” (May 2018), p. 6-7, White Paper, online: <http://www3.weforum.org/docs/WEF_Addressing_E-Payment_Challenges_in_Global_E-Commerce_clean.pdf>, accessed 24 January 2020.

> a payment service supplier that processes transactions and conducts transfers is not performing the same functions as a financial services entity that makes loans from customer deposits. An active and engaged approach from regulators around e-payment innovations can lead to regulatory frameworks that are sound and also drive financial inclusion. Increasingly complex regulation and compliance procedures can result in e-payment or other financial service suppliers "de-risking" – which has a clear knock-on impact on the poorest parts of the population. Further, from a cross-border perspective, efforts could be made to standardize risk-based models. A group of countries could, for example, align on the risk threshold below which simplified due diligence KYC measures would apply.

In effect, while the first principle stands on its own, it also serves as an umbrella for all of the other principles. Accordingly, this Guide focuses on the first principle, both on its own as well as in its role as an umbrella for the other principles. A detailed analysis of each of the other principles is outside the scope of the present discussion. It should, however, be added that the last four principles – namely, technological neutrality, wide access, and risk-based policies and regulations – are linked in their encouragement of innovation. For their part, risk-based policies and regulations also foster safety.

CHAPTER 3 SOUND LEGAL AND REGULATORY FRAMEWORKS FOR E-PAYMENTS: RISK OF LEGAL UNCERTAINTY

The elimination of legal uncertainty in the smooth operation of the payment system has been a stated goal of policymakers. Thus, in its report on core principles for Systematically Important Payment Systems (hereafter: 'SIPS Report'), the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlement (BIS) identified legal risk as one of five types of risks that can arise in payment systems and disrupt their operation.[52] To meet such a risk, Core Principle I requires a systematically important payment system to have 'a well-founded basis under all relevant jurisdictions.'[53]

Subsequently, BIS went further in its 2006 Report titled General Guidance for National Payment System Development (GGNPSD Report). In this report, BIS endorsed the promotion of legal certainty through the development of a transparent, comprehensive, and sound legal framework for the payment system as a guideline for a national payment system development.[54] Having characterized the national payment system as 'one of the principal components of a country's monetary and financial system' to be 'crucial to a country's economic development,' the GGNPSD Report defined a national payment system as 'the configuration of diverse institutional arrangements and infrastructures that facilitates the transfer of monetary value between … parties.'[55] The system consists of cash payments (effectively made in banknotes and coins) and non-cash payments. The latter is said to 'typically involve a complex process of money transfers from the deposit (or credit) account of the payer at one financial institution to the account of the payee at another financial institution.'[56]

It is in this context that the GGNPSD Report explains that '[t]he legal framework for a national payment system is the body of law which determines the rights and obligations of parties in the system.'[57] Hence, reference is specifically made to (i) all parties participating in a payment system, including the payer and payee; (ii) all types of payment systems, rather than only systemic important ones; and (iii) a framework not limited to either safety and efficiency or settlement default risks.

Payment law subject matters

Overview

A comprehensive, and yet specific, payment law thus ought to be multifaceted. An underlying assumption is the existence of a sound legal system containing solid laws addressing subjects such as contract, property, credit, secured credit and insolvency, as well as solid and reliable mechanisms for the administration of justice and dispute resolution. Furthermore, an assumption is to be made as to the existence of effective financial regulation addressing central banking, financial institutions, and markets. Finally, to be assumed is the existence of clear currency laws establishing an official currency, providing for legal tender, and possibly regulating the use of foreign currency. With all of this taken to exist, the focus of the present discussion is on specific laws addressing non-cash payments, namely those payments which are not exclusively in cash. The emphasis is on institutions and transactions.

Thematically, payment law may be divided as follows:

---

[52] CPSS, "Core Principles for Systematically Important Payment Systems" (Basel: BIS, January 2001) at 5, online: <https://www.bis.org/cpmi/publ/d43.pdf>, accessed 24 January 2020.

[53] *Ibid* at 3.

[54] CPSS, "General Guidance for National Payment System Development" (Basel: BIS, January 2006), at 5, 38-42 (Guideline 10) and 63-67 (Annex 4), online: <https://www.bis.org/cpmi/publ/d70.pdf>, accessed 24 January 2020.

[55] *Ibid* at 7.

[56] *Ibid*.

[57] *Ibid* at 38.

- Payment system law governing the regulation and oversight of core interbank clearing and settlement systems;

- Payment transactions law governing rights and remedies of all participants from end-to-end in carrying out a payment transaction; and

- Payment services law governing (i) the regulation and oversight of providers of payment services which are not regulated financial institutions, as well as (ii) rights and remedies of end-participants of a payment transaction, namely, the payer and payee, vis-à-vis the payment service provider with which the end-participant is in privity. The latter aspect overlaps with a portion of payment transactions law. However, it is not limited to the rights and remedies of end-participants towards their payment service providers and also addresses rights and remedies of and towards intermediaries in the payment transactions. At the same time, in contrast to payment transactions law, which covers only the payment transaction itself, payment services law covers the broader contractual relationship between end-parties and their respective payment service providers within which payment transactions are carried out.

However, this classification is not cast in stone. For example, the Singapore Payment Services Act 2019 (No. 2 of 2019) is stated to be '[a]n Act to provide for the licensing and regulation of payment service providers, the oversight of payment systems, and connected matters … '[58] The Act empowers the Monetary Authority of Singapore (MAS) – being the central bank – to address key risks such as money laundering and terrorist financing, loss of funds owed to consumers or merchants due to insolvency, fragmentation and limitations to interoperability, and technology and cyber risks. In addition to providing a licensing framework for payment service providers, the statute addresses the designation framework for significant payment systems.[59]

Pragmatically then, it may be preferable to address payment law as consisting of the following more or less distinct components:

- The organization and operation of clearing and settlement systems, particularly those which are the main engine of the national payment system;

- The identification of policy objectives and/or the policy-setting body for payment systems in general, particularly the national systems;

- Risk to economic and financial activity incurred in connection with carrying out payment transactions;

- The licensing or regulation of payment service providers which are not regulated financial institutions, particularly unregulated deposit takers; and

- Rights and remedies of participants in a non-cash payment transaction.

Among developing nations, a statute addressing all such components other than the fifth one pertaining to rights and remedies of participants in non-cash payment transactions is the Payment and Settlement Systems Act No 28 of 2005 of Sri Lanka.[60] Part III of the 2005 Act addresses systemic risk. In turn, Part II of the Act:

- Designates the Central Bank as the regulator and supervisor of the payment system, as well as assigns to it a leading role in overseeing its development. The Central Bank may provide interbank

[58] Singapore Payment Services Act 2019 (No. 2 of 2019) <https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220#P12-P22-P31->, accessed 24 February 2020. The quote is from the preamble to the Act.

[59] See in general, Monetary Authority of Singapore, "Explanatory Brief on the Payment Services Bill",(19 November 2018), online: <https://www.mas.gov.sg/news/speeches/2018/explanatory-brief-on-the-payment-services-bill>, accessed 24 February 2020.

[60] Payment and Settlement Systems Act, No. 28 of 2005, online: <https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/acts/en/Payment_setttlement_sys_act.pdf>, accessed 24 January 2020. See: Benjamin Geva, "Payment System Modernization and Law Reform in Developing Nations: Lessons from Cambodia and Sri Lanka" (2009), 126 Banking LJ 402.

clearing services, assist in their establishment, or oversee them. Payment system policy and risk control are brought under the authority of the Central Bank. In addition, the Central Bank is assigned responsibility and role in connection with securities settlement systems, securities accounts, and the central depository for securities.

- Further recognizes the involvement of non-bank players in the payment system. Part II authorizes the Central Bank to regulate, supervise, and oversee providers of money services, including cheque cashers, currency bureaus, and money transmitters. To that end, the Central Bank is authorized to require the licensing or registration of money services providers.

- Authorizes the Central Bank to regulate, supervise, and oversee payment systems; identify individual payment systems and designate them for further regulation; scrutinize rules of designated systems and issue further directives regarding access to, participation in, as well as the operation of, a designated payment system, its interaction with other payment systems, and its relationship with its participants.

Legislation comprehensively addressing the fifth aspect, dealing with rights and remedies in a non-cash payment transaction, is the Negotiable Instruments and Payment Transactions Act 2005 of Cambodia.[61] Chapter V of the Act covers non-cash payments carried over through the banking systems, executed in either electronic or paper-based systems. It is premised on modern statutory sources, such as the Model Law on International Credit Transfers (MLICT) developed by the United Nations Commission on International Trade Law (UNCITRAL)[62] and incorporates rules based on widely-accepted banking practices in developed countries. It was introduced to enhance legal certainty in an environment dominated by banking and legal systems, which required both guidance to develop sound practices and maintenance of traditions.

A payment transaction governed by Chapter V denotes the transfer of funds between two bank accounts. It is initiated by a payment order issued by a bank customer. Payment transactions governed by Chapter V are debit and credit transfers,[63] in-house and interbank payments, whether domestic or international, in either local or in foreign currency. Chapter V provides for a legal framework that will facilitate the introduction of (i) electronic banking on both the retail and wholesale level, (ii) preauthorized payments, and (iii) a large-value transfer system for payments in international and domestic financial and interbank markets. Chapter V provides for rights and remedies of participants in the payment system, including the interbank settlement. It also covers fundamentals relating to the bank and customer relationship evolving around the bank account.

Chapter V further takes account of, and thus provides a firm legal basis for, the role of the National Bank of Cambodia in the payment system, particularly as provider of the final interbank settlement and institution responsible for the safety and security, as well as future development, of the payment system in Cambodia. Chapter V also provides for the legal framework needed to implement the BIS Core Principles for Systematically Important Payment Systems.

The following discussion addresses each of the five aspects of a multifaceted payment law system identified in the section above.

The national payment system: organization, operation, policy setting

First, payment laws ought to address the organization and operation of the national payment system. Such laws will govern the framework for the operation of clearing and settlement.

Second**,** payment laws must identify the policy-setting body for payment systems. Typically, this may be the central bank, albeit it may also be a joint body involving additional financial regulators and possibly payment system participants and stakeholders. Some countries may confer a policy-making role to a broadly based

[61] Law on Negotiable Instruments and Payment Transactions, online: <http://www.cambodiainvestment.gov.kh/wp-content/uploads/2011/09/Law-on-Negotiable-Instruments-and-Payment-Transaction_051024.pdf>, accessed 24 January 2020. See Benjamin Geva, "Payment System Modernization", ibid. .

[62] Model Law on International Credit Transfers, G.A. Res. 47/34, art. 6(b), U.N. Doc. A/RES/47/34 (Feb. 9, 1993).

[63] The distinction is discussed in the introductory section of the Appendix, infra.

payments council, empowering it with advisory powers at the very least. As well, the law may either address policy objectives or leave them to the consideration of the policy-setting body. Issues to be addressed under these two first subjects are regulatory. They include general topics of oversight and supervision, governance, architecture and design, access, payment systems operating outside the national system, the role or level of involvement of entities that have not been subject to (and may remain outside) traditional financial regulation, the right balance between co-operation and competition, customer protection, and autonomy of participants and their organizations. It is within this framework that the relationships among the various financial regulators, as well as among competing and complementary objectives of financial regulation, are to be addressed. Particular attention in this context is to be given to the role of the central bank by reference to that of regulators of financial institutions and financial markets.

Risk, licensing, registration, regulation

A third subject to be dealt with is the risk to economic and financial activity. For example, Canadian legislation[64] distinguishes between 'payment system risk' and 'systemic risk', with only the first being relevant for a retail payment system:

Thus:

> *payments system risk* means the risk that a disruption to, or a failure of, a clearing and settlement system could cause a significant adverse effect on economic activity in Canada by
>
> (a) impairing the ability of individuals, businesses or government entities to make payments, or
>
> (b) producing a general loss of confidence in the overall Canadian payments system, which includes payment instruments, infrastructure, organizations, market arrangements and legal frameworks that allow for the transfer of monetary value.

On the other hand:

> *systemic risk* means the risk that the inability of a participant to meet its obligations in a clearing and settlement system as they become due, or a disruption to or a failure of a clearing and settlement system, could, by transmitting financial problems through the system, cause
>
> (a) other participants in the clearing and settlement system to be unable to meet their obligations as they become due,
>
> (b) financial institutions in other parts of the Canadian financial system to be unable to meet their obligations as they become due,
>
> (c) the clearing and settlement system's clearing house or the clearing house of another clearing and settlement system within the Canadian financial system to be unable to meet its obligations as they become due, or
>
> (d) an adverse effect on the stability or integrity of the Canadian financial system.

A specific aspect of this subject is the risk presented by a network of money transmitters such as mobile payment operators. What moves in such networks between customers is e-money – with funds on deposit with banks moving only among the mobile operator/money transmitter in settlement of payment between customers of different institutions.

The fourth aspect is the licensing or regulation of payment service providers that are not regulated financial institutions. Competition and innovation are likely to be enhanced by opening the field of provision of payment services to money transmitters. Such institutions are to be made subject to light regulation designed to prevent misuse for illegal purposes and misuse by violating customers' rights. In this framework, attention is

[64] Payment Clearing and Settlement Act SC 1996, c 6, Sch s 2.

to be given primarily to service providers positioned in privity with the end parties – that is, either the payer or the payee. Aspects to be addressed are registration and/or licensing; capital, investment powers, ownership, and governance.

As an example of the fourth aspect, Art. 1(1) of the Second Payment Services Directive of the European Union (PSD2 or Directive)[65] enumerates six categories of payment service provider (PSP):

(a) credit institutions as defined in point (1) of Art. 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council,[66] including branches thereof within the meaning of point (17) of Art. 4(1) of that Regulation where such branches are located in the Union, whether the head offices of those branches are located within the Union or, in accordance with Art. 47 of Directive 2013/36/EU and with national law, outside the Union;

(b) electronic money institutions within the meaning of point (1) of Art. 2 of Directive 2009/110/EC, including, in accordance with Art. 8 of that Directive and with national law, branches thereof, where such branches are located within the Union and their head offices are located outside the Union, in as far as the payment services provided by those branches are linked to the issuance of electronic money;

(c) post office giro institutions which are entitled under national law to provide payment services;

(d) payment institutions;

(e) the ECB and national central banks when not acting in their capacity as monetary authority or other public authorities;

(f) Member States or their regional or local authorities when not acting in their capacity as public authorities.

Among the various PSPs, the Directive regulates payment institutions.[67] Most of Title II dealing with 'Payment Service Providers' is dedicated to their regulatory aspects, such as licensing and capital requirements, which are not to be set out in detail in the present discussion. Activities permitted for payment institutions are enumerated in Art. 18(1) of the Directive. Apart from the provision of payment services, such activities are

> (a) the provision of operational and closely related ancillary services such as ensuring the execution of payment transactions, foreign exchange services, safekeeping activities, and the storage and processing of data; (b) operating payment systems…; and (c) business activities other than the provision of payment services, having regard to applicable Union and national law.[68]

Payment institutions are authorized to execute transactions in electronic money, but not to issue it.[69]

---

[65] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing 2007/64/EC, 2015 O.J. (L 337) 35, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366>, accessed 24 January 2020.

[66] 'Credit institution' is defined to mean 'an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.' Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No 648/2012, art. 4(1), 2013 O.J. (L 176) 1, 18. Effectively, it is a commercial bank.

[67] PSD2 titlesec II, Chapter 1.

[68] PSD2 Art. 18(1). The fourth category replaced Art. 10(3) of the Proposal to the original PSD, under which permitted activities 'shall not be restricted to payment services, having regard to the applicable national and Community law.' Implementing the Community Lisbon Programme: Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market and Amending Directive 97/7/EC, and 2002/65/EC (presented by the Commission) COM (2005) 603 final (Dec. 1, 2005), [hereinafter Lisbon Programme Proposal] Art. 10(3).

[69] PSD2, preamble, paragraph 25.

Specific provisions cover the capital requirements of payment institutions.[70] They address safeguarding through segregation of funds placed for payment transactions;[71] the authorization process, the maintenance as well as the withdrawal of authorization, and the registration of authorized payment institutions;[72] compliance with accounting and statutory audit requirements;[73] the use of branches and third-parties by payment institutions;[74] record-keeping requirements;[75] and professional secrecy.[76] They also provide for the designation of competent authorities[77] for prudential regulation and supervision as well as their activities and exchange of information[78] and right to apply to the courts.[79]

Other payment services relate to payment initiation and account information.[80] Payment initiation service (PIS) is defined in Art. 4(15) of the Directive as 'a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.' Account information service (AIS) is defined in Art. 4(16) as 'an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.' A provider of such services is respectively a payment initiation service provider (PISP) or an account information service provider (AISP).[81] The Directive covers both services, even to the extent that they may be viewed as 'technical service providers', which provide services supporting 'the provision of payment services, without them entering at any time into possession of the funds to be transferred.'[82] Such services are otherwise excluded from the application of the Directive, as specified under Art. 3(j). While the Directive does not enumerate PISPs and AISPs as PSPs, they provide payment services and are treated as payment institutions, which of course are PSPs.[83]

A circular letter on licensing procedures and requirements related to payment system transactions issued by Bank Indonesia (BI) is a good example of a regulatory instrument addressing payment services providers. BI Circular Letter No. 18/41/DKSP regarding the 'Implementation of Payment Transaction Processing', dated 30 December 2016 (the Circular Letter), implements BI Regulation No. 18/40/PBI/2016 on the 'Implementation of Payment Transaction Processing' (BI Regulation No. 18/40/PBI/2016), which was issued on 9 November 2016. The Circular Letter mainly concerns licensing procedures and requirements set by BI for various payment system service providers, such as (i) principals, (ii) switching providers, (iii) issuers, (iv) acquirers, (v) payment gateway providers, (vi) clearing providers, (vii) final settlement providers, (viii) fund transfer providers and (ix) electronic wallet (e-wallet) providers. It also refers to supporting providers, as defined in BI Regulation No. 18/40/PBI/2016, which support payment system service providers in processing payments.[84]

An important aspect of the regulation dealing with money transmitters is the safety of, or protection to be given to, customers' funds in the case of insolvency of a money transmitter. According to general insolvency laws, funds in transit, or held by such institutions, including either in anticipation of receiving customer-payers' payment instructions or before releasing them to payees, are not protected in case of an institution's insolvency. Stated otherwise, a public deposit insurance scheme typically covers only funds held in banks or other regulated deposit-taking or financial institutions but not money transmitters. This means that upon

[70] Art. 7-9 provide for initial capital, own funds, and two alternative methods for calculation of own funds.

[71] PSD2 Art. 10.

[72] PSD2 Arts. 5, 11-14, 16.

[73] PSD2 Art. 17.

[74] PSD2 Arts. 19-20.

[75] PSD2 Art. 21.

[76] PSD2 Art. 24.

[77] For the designation of "competent authorities…to ensure and monitor effective compliance with the Directive,", See PSD2 Art. 100.

[78] PSD2 Arts. 22-23.

[79] PSD2 Art. 25.

[80] Points 7 and 8, respectively in PSD2 Annex I.

[81] PSD2 Arts. 4(18) and (19), respectively.

[82] PSD2 Art. 3(j).

[83] PSD2, preamble, paragraph 26.

[84] See SSEK Indonesian Legal Consultants , "Bank Indonesia Issues Rules for Payment System Service Providers" (March 30 2017), online: <https://www.lexology.com/library/detail.aspx?g=c539f4a6-d18f-4913-a835-131a9d9031f6>, accessed 24 January 2020.

the failure of a bank in which the money transmitter holds customer's funds, the direct beneficiary of the insurance is the money transmitter, not its customers. The transmitter's customer is likely, however, to benefit indirectly from the protection given to the money transmitter as a customer of the failing bank. At the same time, the insolvency of a money transmitter holding customers' funds in a bank is treated as insolvency of a bank customer – in which case the transmitter's funds (consisting of funds given by its own customers), on deposit at the bank, are distributed among all the money transmitter's creditors, rather than refunded to the transmitter's payment customers. Unless such funds are treated as held at a bank by the money transmitter in trust in favour of its own customers, these customers require the adoption of a specific statutory scheme, such as public deposit insurance, that protects them directly as if the money transmitter were a bank.

The third and fourth aspects are conceptually distinct. The fourth aspect (payment service provider (PSP) regulation) addresses both customer protection and prudential regulation. The third one (default of a participant in a payment and settlement system) is concerned with the risk that may be posed to the economic and financial systems of the payment system in which the PSP takes part. Access to a payment system is a topic falling between the two aspects. Regardless, in the context of both the third and fourth aspects, payment laws ought to confer on the authorities, possibly the central bank (or the Minister of Finance), the powers to regulate, license, supervise, and oversee:

- **Payment systems**, including the designation of identified individual ones for further regulation, and for which rules are to be scrutinized and directives regarding access to, participation in, as well as the operation of, as well as interaction with other payment systems and with its participants, may be issued.

- **Providers of money or payment services**, including cheque cashers, currency bureaus and money transmitters.

Payment transactions: rights and remedies

The fifth aspect deals with rights and remedies of participants in a non-cash payment transaction. A non-cash payment can broadly be defined as any mechanism for the transfer of monetary value over the payment system. Certainly, the reliability of a system in generating a method for discharging debts in a timely and secure fashion requires a clear definition of its various components. Overall, laws relating to this subject ought to cover cheques and negotiable instruments, debit transfers, and credit transfers. They are to cover payment transactions carried out in both paper-based and electronic systems, whether processed in bulk or individually, whether they are retail or large-value/wholesale systems, and whether they settle in DNS or RTGS systems. They ought also to address transparency and disclosures, particularly to consumers, of terms and costs.

In the context of this fifth subject, legislative solutions are designed to meet the legal uncertainty risk in payments by providing a comprehensive legal framework to govern the rights and remedies of participants in a payment transaction.

According to the GGNPSD Report, '[a] sound legal framework for the national payment system reduces the legal uncertainty and risk for participants in payment infrastructures and service markets.'[85] In connection with credit transfers, the GGNPSD Report further states that the applicable law ought to 'authorize paper-based credit transfers and electronic wire transfers' as well as to 'govern such aspects as finality of payment, misdirected payments, payment fraud and availability of funds to the customer.' Such subjects 'may be governed by contract and common law to some extent but legislation is desirable.'[86]

In line with the on-going global trend,[87] this Guide endorses the desirability of specific legislation. Briefly stated, in the modern era, on-going technological enhancements significantly increased the use and benefits of the credit transfer. In turn, traditional payment instrument legislation, which focused on the paper-based

[85] GGNPSD Report, supra n 54 at 38.

[86] *Ibid* at 63.

[87] See Payment Systems Worldwide, supra n 6 at 61.

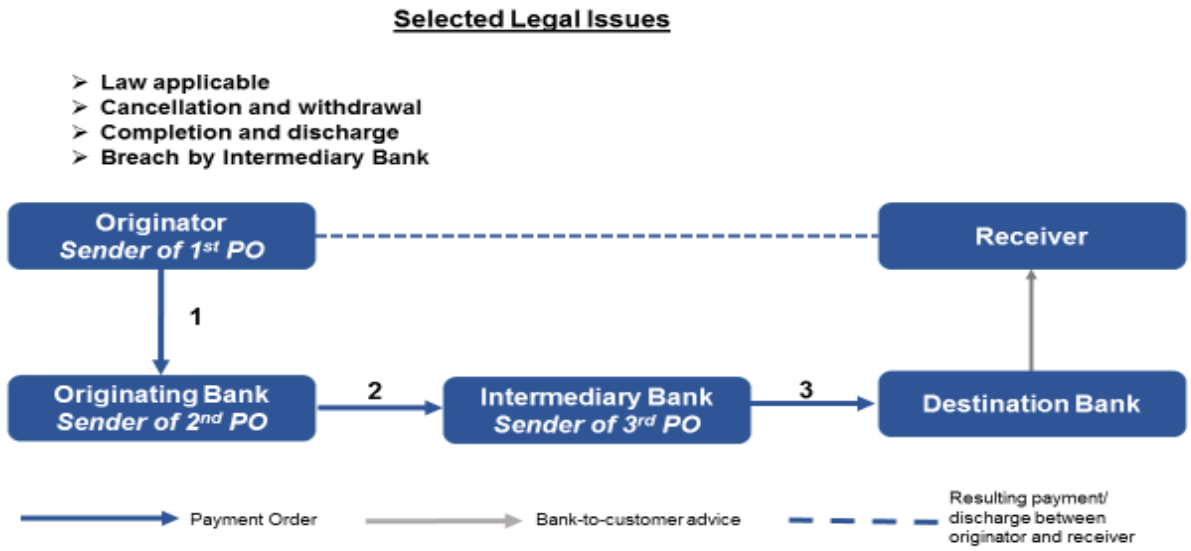
negotiable instruments used in debit transfers, has become inadequate to deal with electronic payment transactions. General principles of law, though available, are slow to develop, such that reliance on them does not secure certainty and predictability.[88] A contract is not an effective mechanism to provide for the rights of third parties; the same is true for interbank payment system rules. As well, a series of bilateral contracts is unlikely to produce harmonization. Finally, between bank and customer, contracts may be one-sided, unfair to customers, and thus, in some cases, risk lack of enforceability on public policy grounds.

Topics to be addressed by payment transactions legislation cover payment orders, third-party processors, completion of credit transfer and discharge, completion of the debit transfer and discharge, mistaken or fraudulent payments: liability, damages and restitution, and accounts. Specific issues to be addressed are:

- Scope;
- The payment order and its acceptance or rejection;
- Timely cancellation and automatic withdrawal of an (unexecuted) payment order;
- Sender's payment obligation and its excuse under "money-back guarantee" upon non-completion of a credit transfer;
- Sender's payment;
- Sender's liability;
- Fraudulent and mistaken (albeit authorized) payment orders;
- Finality of payment: completion of credit transfer and discharge of underlying debt;
- Liability for losses by a Receiving Bank;
- Restitution upon erroneous completion of credit transfers;
- Third-party Intermediaries;
- Law applicable: variations and cross-border – international setting.

[88] For my own analysis of the area under common law and civil codes, see Benjamin Geva, Bank Collections and Payment Transactions – Comparative Study of Legal Aspects (Oxford: Oxford University Press, 2001) at 186-317.

Figure 9 Selected legal issues



For a detailed analysis by reference to two leading statutes enacted in developed countries, see the Appendix.

Concluding Observations

It is not suggested that all subject matters of payment law need necessarily be included in one statute. To begin with, as a matter of local constitutional law, payment law is unlikely to be a specific branch of legislative power. Accordingly, in federal countries, some aspects of payment law may fall into the powers of the federal entity and others into those of the federation units. Additionally, unitary jurisdictions may prefer to separate between regulatory and private law aspects and address them through different statutes. Furthermore, and more generally, certain aspects are susceptible to delegation to an administrative authority to be passed as regulations rather than determined specifically by a statute of the legislature. Finally, matters such as the organization of the clearing and settlement system may be entrusted to the hands of industry organizations regardless of whether they are established by law. Resolution of these aspects may vary from place to place and is outside the scope of this Guide but a few examples are given below.

In Canada, the Payment Clearing and Settlement Act[89] addresses risk in clearing and settlement systems. For its part, the Canadian Payments Act[90] covers the Canadian Payments Association and its powers, particularly in relation to national systems for clearing and settlement, as well as the Minister of Finance's powers to designate and regulate payment systems of national scope. Another Canadian statute is the Payment Card Networks Act,[91] which is designed to regulate national payment card networks. That statute addresses the bilateral relationship of a card network operator with the card issuer as well with the acquirer. Section 5 of the Payment Card Networks Act provides the Financial Consumer Agency of Canada, established under section 3 of the Financial Consumer Agency of Canada Act,[92] the mandate to supervise the payment card network.

[89] SC 1996, c 6, Sch.

[90] RSC 1985, c C-21.

[91] SC 2010, c 12, s 1834.

[92] SC 2001, c 9.

In South Africa, the central bank South Africa Reserve Bank (SARB), provides the only inter-bank settlement system[93] and under section 10 of the South African Reserve Bank Act 90 of 1989,[94] is entrusted with the leadership of payment system developments. The National Payment System Act 78 of 1998[95] confirms this power in section 2 and sets out in section 3, with regard to a payment system management body, its relationship with the SARB and the restricted access to the SARB's settlement facilities. Section 4A of the 1998 Act addresses risk.

In Australia,

> … payment system providers are overseen by three regulators: the Australian Securities and Investments Commission … is responsible for ensuring consumer protection and market integrity in payment systems; the Australian Prudential Regulation Authority … is responsible for supervising the safety and soundness of financial institutions whose activities give rise to liabilities in the payments system; and the Payments System Board … of the Reserve Bank of Australia … is responsible for ensuring systemic stability as well as efficiency and competition in the payment system.[96]

[93] CPSS, "Payment, clearing and settlement in South Africa" in Red Book (Basel: BIS, 2012) at §3.1, online: <https://www.bis.org/cpmi/publ/d105_za.pdf>, accessed 24 January 2020.

[94] Act 90 of 1989 As amended by Transfer of Powers and Duties of the State President Act 51 of 1991, Safe Deposit of Securities Act 85 of 1992, South African Reserve Bank Amendment Act 10 of 1993, General Law Third Amendment Act 129 of 1993, South African Reserve Bank Amendment Act 2 of 1996, South African Reserve Bank Act 39 of 1997, South African Reserve Bank Amendment Act 57 of 2000, and Exchange Control Amnesty and Amendment of Taxation Laws Act 12 of 2003.

[95] Act 78 of 1998 (NPSA), as amended by National Payment System Amendment Act 22 of 2004, National Credit Act 34 of 2005, Co-operative Banks Act 40 of 2007, and Financial Services Laws General Amendment Act 22 of 2008.

[96] Australian Government Productivity Commission, Business Set-up, Transfer and Closure: Productivity

Commission Draft Report (May 2015) at 196 (§9.1), online: <http://www.pc.gov.au/inquiries/current/business/draft>, accessed 24 January 2020.

CHAPTER 4 E-PAYMENTS SERVICES (EPS) UNDER INTERNATIONAL TRADE LAW

This chapter addresses the application of international trade law to electronic payment services (EPS). Certainly, in the absence of an international agreement, a country is free to preclude foreign entities from providing EPS within its borders, and in allowing access to foreign entities, a country is free to burden them with discriminatory restrictions. Against this background, this chapter examines prominent international trade agreements and addresses rights and obligations of countries signatories to them to facilitate, restrict or block the provision of EPS by foreign entities. In case of permissible restrictions, an issue arises as to whether foreign and domestic service providers may be subject to different regulatory treatment. In principle, international trade agreements purport to ensure equitable treatment in accessing foreign markets and the promotion of progressive liberalization of trade leading to the elimination of trade barriers**.**

EPS under the GATS

The General Agreement on Trade in Services (GATS)[97] is the first multilateral agreement covering trade in services. It was negotiated during the last round of multilateral trade negotiations, referred to as the Uruguay Round, and came into force in 1995. The GATS provides a framework of rules governing services trade, establishes a mechanism for countries to make commitments to liberalize trade in services, and provides a mechanism for resolving disputes between countries. It is designed to ensure equitable access to the market, as well as promote progressive liberalization of trade in services.[98] Members' obligations under the GATS apply only to trade in those services sectors for which Members have voluntarily assumed obligations by inscribing commitments in their Schedule of Specific Commitments. Financial services are listed under the GATS as a sector[99] covering 'banking and other financial services'.[100] They include "all payment and money transmission services."[101]

GATS Part III, consisting of Arts. XVI-XVIII, addresses subject matters for specific commitments to be undertaken by a Member with regard to a selected sector. The subject matters are market access and national treatment, though there may also be additional commitments. Under Art. XX, the specific commitments relating to such matters must be set out in a schedule annexed to the GATS and shall form an integral part thereof. Under Art. VI (1),

> In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner.[102]

GATS Art. XVI addresses market access as follows:

> 1. With respect to market access through the ***modes of supply*** identified in Article I, each Member shall accord services and service suppliers of any other Member treatment ***no less favourable***

[97] GATS, World Trade Organization (WTO) online: <https://www.wto.org/english/docs_e/legal_e/26-gats.pdf>, accessed 24 January 2020.

[98] See e.g. Backgrounder on the GATS, Government of Canada, online <https://www.international.gc.ca/trade-agreements-accords-commerciaux/wto-omc/gats-agcs/back-info.aspx?lang=eng>, accessed 24 January 2020.

[99] Sector-by-sector information, WTO, online: <https://www.wto.org/english/tratop_e/serv_e/serv_sectors_e.htm>, accessed 24 January 2020.

[100] Financial services, WTO, online: <https://www.wto.org/english/tratop_e/serv_e/finance_e/finance_e.htm>, accessed 24 January 2020.

[101] Background on financial services, WTO, online: <https://www.wto.org/english/tratop_e/serv_e/finance_e/finance_intro_e.htm>, accessed 24 January 2020.

[102] These provisions are discussed by Panagiotis Delimatsis, "The Interaction Between GATS Articles VI, XVI, XVII and XVIII after the US – Gambling Case," nccr trade regulation, Working Paper No 2006/9, June 2006, online: <https://www.researchgate.net/publication/228157455_The_Interaction_between_GATS_Articles_VI_XVI_XVII_and_XVIII_after_the_US_-_Gambling_Case>, accessed 24 January 2020.

than that provided for under the terms, limitations and conditions agreed and specified in its Schedule.

2. In sectors where market-access commitments are undertaken, the measures which a Member shall **not** maintain or adopt either on the basis of a regional subdivision or on the basis of its entire territory, unless otherwise specified in its Schedule, are defined as:

   (a) limitations on the **number of service suppliers** whether in the form of numerical quotas, monopolies, exclusive service suppliers or the requirements of an economic needs test;

   (b) limitations on the **total value of service transactions or assets** in the form of numerical quotas or the requirement of an economic needs test;

   (c) limitations on the **total number of service operations or on the total quantity of service output** expressed in terms of designated numerical units in the form of quotas or the requirement of an economic needs test;

   (d) limitations on the **total number of natural persons that may be employed** in a particular service sector or that a service supplier may employ and who are necessary for, and directly related to, the supply of a specific service in the form of numerical quotas or the requirement of an economic needs test;

   (e) measures which restrict or require **specific types of legal entity** or joint venture through which a service supplier may supply a service; and

   (f) limitations on the **participation of foreign capital in terms of maximum percentag**e limit on foreign shareholding or the total value of individual or aggregate foreign investment.

[Emphasis added]

Modes of supply identified in GATS Art. I(2)(c), to which Art. XVI(1) refers, are cross border supply, consumption abroad, commercial presence, and presence of natural persons.[103]

The primary focus of obligations and rules under GATS Art. XVI is the provision of non-discriminatory quantitative restrictions impeding access to markets. Restricting market access other than quantitatively does not fall under Art. XV. In this context, the World Trade Organization (WTO) Panel report in US – Gambling (2004)[104] held that a total prohibition on the cross-border supply of a service in respect of which a full market access commitment was undertaken is deemed a market access limitation falling under Art. XVI: 2(a) and (c). This is so even if the prohibition does not contain any express reference to numbered units. Stated otherwise, zero access is a quantitative measure under Art. XVI. In the final analysis, a full market access commitment in a given sector cannot co-exist with market access limitations in the same service sector that exhibits a numerical or quantitative nature and this is regardless of the form taken by these measures.

A country may, however, determine limitations on market access for each committed sector and mode of supply, as per national treatment, governed by Art. XVII providing as follows:

1. In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment ***no less favourable*** than that it accords to its own like services and service suppliers.

[103] For elaboration see <https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm> under #4, accessed 24 January 2020.

[104] DS285: United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services, online: <https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm>, accessed 24 January 2020, and see: Isaac Wobl, "The Antigua-United States Online Gambling Dispute" (July 2009) United States International Trade Commission Journal of International Commerce and Economics, Web Version: <https://www.usitc.gov/publications/332/journals/online_gambling_dispute.pdf>, accessed 24 January 2020.

2. A Member may meet the requirement of paragraph 1 by according to services and service suppliers of any other Member, either formally identical treatment or formally different treatment to that it accords to its own like services and service suppliers.

3. Formally identical or formally different treatment shall be considered to be less favourable if it modifies the conditions of competition in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member.

[Emphasis added]

Additional Commitments are dealt with Art. XVIII, providing as follows:

- Members may negotiate commitments with respect to measures affecting trade in services not subject to scheduling under Arts. XVI or XVII, including those regarding qualifications, standards or licensing matters. Such commitments shall be inscribed in a Member's Schedule.

Measures affecting electronic payment services (EPS) in alleged violations of GATS Arts. XVI and XVII were dealt with by the WTO Panel addressing the United States' request of 11 February 2011 with respect to 'certain restrictions and requirements maintained by the People's Republic of China pertaining to EPS for payment card transactions and the suppliers of those services'.[105] The United States alleged that China permits only a Chinese entity, China UnionPay (CUP), to supply electronic payment services for payment card transactions denominated and paid in the official currency of China, renminbi (RMB) in China. Service suppliers of other WTO Members can only supply these services for payment card transactions paid in foreign currency. The United States further alleged that:

- China also requires all payment card processing devices to be compatible with CUP's system, and that payment cards must bear its logo;

- CUP has guaranteed access to all merchants in China that accept payment cards, while services suppliers of other Members must negotiate for access to merchants.

As to the scope of China's GATS Commitments, the Panel found that China's Schedule did not include a cross-border mode of supply market access commitment to allow the supply of EPS into China by foreign EPS suppliers. However, the Panel held that China's Schedule included a market access commitment that allows foreign EPS suppliers to supply their services through commercial presence mode of supply in China, so long as a supplier meets certain qualifications requirements related to local currency business. As well, China's Schedule contained a full national treatment commitment for the cross-border supply of EPS mode of supply. It also contained a commitment under the commercial presence mode of supply that is subject to certain qualifications requirements related to local currency business.

With regard to the GATS market access obligation, the Panel found that:

- There was no evidence that China maintains CUP as an across-the-board monopoly supplier for the processing of all domestic RMB payment card transactions, in breach of its obligations under Art. XVI;

- At the same time, China acted inconsistently with GATS Art. XVI: 2(a) in view of its market access commitment in relation to the commercial presence mode of supply by granting CUP a monopoly for the clearing of certain RMB payment card transactions. This finding was made on the basis that only CUP may clear RMB-denominated transactions involving RMB payment cards issued in China and used in Hong Kong or Macao, or RMB cards issued in Hong Kong or Macao used in China.

[105] DS413: China – Certain Measures Affecting Electronic Payment Services, online: <https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds413_e.htm>, accessed 24 January 2020. For a detailed discussion see Arvind Rattan, "The Liberalization of Electronic Payment Services in the Multilateral Framework on Trade Services" (2013) Master thesis supervised by P. Delimatsis, Tilburg University, online: <http://arno.uvt.nl/show.cgi?fid=132833>, accessed 24 January 2020.

Regarding the GATS national treatment obligation under GATS Art. XVII, the Panel found that requirements, such as that:

- All bank cards issued in China must bear the logo of CUP's network and be interoperable with that network;
- All terminal equipment in China must be capable of accepting that logo cards; and
- Acquirers of transactions for payment card companies post that logo and be capable of accepting payment cards bearing that logo,

are each inconsistent with China's national treatment obligations under Art. XVII.

This is so because, contrary to China's national treatment commitments, relating to the cross-border supply and commercial presence, these requirements modified the conditions of competition between EPS suppliers of other Members and China's own like services and service supplier CUP to the detriment of those other EPS suppliers.

EPS under a free trade agreement

E-payments are specifically addressed by the Agreement between the United States of America, the United Mexican States and Canada (USMCA),[106] which is the only free trade agreement to be addressed in this Guide.

To begin with, USMCA Art. 19.5 requires parties to 'maintain a legal framework governing electronic transactions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996.' Personal information protection is addressed in Art. 19.8, while paperless trading is encouraged by USMCA Art. 19.9. For its part, USMCA Art. 19.12 provides that:

> No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

Chapter 15 and 17 are more specific in addressing e-payments. The former does it in conjunction with cross-border services and the latter as part of its treatment of financial services.

Under USMCA Art. 15.2 (1), Chapter 15, dealing with cross-border services,

> applies to measures adopted or maintained by a Party relating to cross-border trade in services by a service supplier of another Party, including a measure relating to:
>
> (a) the production, distribution, marketing, sale or delivery of a service;
>
> (b) the purchase or use of, or payment for, a service;
>
> (c) the access to or use of distribution, transport, or telecommunications networks or services in connection with the supply of a service; [or]
>
> (d) the presence in the Party's territory of a service supplier of another Party;

Footnotes to USMCA Art. 15.2(1) clarify that 'subparagraph (a) includes the production, distribution, marketing, sale or delivery of a service by electronic means' and that 'subparagraph (b) includes the purchase or use of, or **payment for, a service by electronic means**' [emphasis added].

[106] Text from 30 May 2019, Signed 30 November 2018, online: <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>, accessed 24 January 2020.

National treatment – that is 'treatment no less favourable than that it accords, in like circumstances, to its own services and service suppliers' – is mandated under Art. 15.3. For its part, most-favoured-nation treatment is required under USMCA Art. 15.5. Limitations on market access and local presence are precluded under USMCA Arts. 15.5 and 15.6 respectively. USMCA Art. 15.9 governs the recognition by 'a Party's standards or criteria for the authorization, licensing, or certification of a service supplier.'

The substantive obligations regarding payments and transfers are addressed in USMCA Art. 15.12 as follows:

1. Each Party shall permit all transfers and payments that relate to the cross-border supply of services to be made freely and without delay into and out of its territory.

2. Each Party shall permit transfers and payments that relate to the cross-border supply of services to be made in a freely usable currency at the market rate of exchange that prevails at the time of transfer.

3. Notwithstanding paragraphs 1 and 2, a Party may prevent or delay a transfer or payment through the equitable, non-discriminatory, and good faith application of its laws that relate to:

   (a) bankruptcy, insolvency, or the protection of the rights of creditors;

   (b) issuing, trading, or dealing in securities or derivatives

   (c) financial reporting or record keeping of transfers when necessary to assist law enforcement or financial regulatory authorities;

   (d) criminal or penal offenses; or

   (e) ensuring compliance with orders or judgments in judicial or administrative proceedings.

Paragraph (3) is supplemented by paragraph (4), under which USMCA Art. 15.12 'does not preclude the equitable, non-discriminatory, and good faith application of a Party's laws relating to its social security, public retirement, or compulsory savings programs.'

USMCA Art. 17 also covers e-payments in dealing with financial services. This is because under USMCA Art. 17.1, financial service is defined to include:

> (h) all payment and money transmission services, including credit, charge and debit cards, travellers checks, and banker's drafts.

National treatment, most-favoured-nation treatment, market access and recognition are respectively addressed in USMCA Arts. 17.3, 17.4. 17.5, and 17.12.

In principle, under Art. USMCA 17.7,

> Each Party shall permit a financial institution of another Party to supply a new financial service that the Party would permit its own financial institutions, in like circumstances, to supply without adopting a law or modifying an existing law.

Under USMCA Art. 17.11(3), without prejudice to 'any other provision of this Agreement that permits a Party to restrict transfers,'

> Notwithstanding … Article 15.12 (Payments and transfers) … a Party may prevent or limit a transfer by a financial institution or a cross-border financial service supplier to, or for the benefit of, an affiliate of or person related to that institution or supplier, through the equitable, non-discriminatory and good faith application of a measure relating to maintenance of the safety, soundness, integrity, or financial responsibility of financial institutions or cross-border financial service suppliers.

Under USMCA Art. 17.15, and without conferring or requiring access to the Party's lender of last resort facilities:

> Under terms and conditions that accord national treatment, each Party shall grant financial institutions of another Party established in its territory access to payment and clearing systems operated by public entities, and to official funding and refinancing facilities available in the normal course of ordinary business. …

Under USMCA Art. 17.18 (2),

> No Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory.

At the same time, under USMCA Art. 17.18(4),

> Nothing in this Article restricts the right of a Party to adopt or maintain measures to protect personal data, personal privacy and the confidentiality of individual records and accounts, provided that these measures are not used to circumvent the commitments or obligations of this Article.

Concluding Observations

To encourage access of global EPS providers, developing countries are encouraged to ensure non-discriminatory access to such providers. As indicated at the beginning of this chapter, Members' obligations under the GATS apply only to trade in those services sectors for which Members have voluntarily assumed obligations by inscribing commitments in their Schedule of Specific Commitments. Financial services are listed under the GATS as a sector covering 'banking and other financial services'. They include 'all payment and money transmission services'[107]—which covers EPS.

A GATS Member State that assumes obligations with respect to the financial services sector is thus restricted in imposing access limitations on foreign EPS providers. Measures taken with regard to EPS may also be governed by a Free Trade Agreement by which a country is bound.

[107] Background on financial services, WTO, online: <https://www.wto.org/english/tratop_e/serv_e/finance_e/finance_intro_e.htm>, accessed 24 January 2020.

CHAPTER 5 CONCLUSIONS

Legislation governing e-payments comprises of two broad areas. One is the area of e-commerce which deals with matters such as validity and reliability of electronic signature and electronic documents that ought to apply to payment instructions and documents. The other area is payment law covering the non-paper environment. Particular areas to be covered are:

- the organization and operation of the national payment system;
- the identification of the policy-setting body for payment systems;
- risk to economic and financial activity;
- the licensing or regulation of payment service providers which are not regulated financial institutions, particularly not regulated deposit takers; and
- rights and remedies of participants in a non-cash payment transaction.

To secure legal certainty, developing nations should adopt comprehensive laws covering all these areas. They should further endeavour to have all such laws harmonized with those of trading partners as well having them consistent with international standards discussed in this Guide. To a large extent the seamless process of payment is enhanced by a harmonized, if not uniform law, that governs it from end to end.

APPENDIX ADDRESSING LEGAL RISK IN CREDIT TRANSFERS BY ART. 4A OF THE AMERICAN UNIFORM COMMERCIAL CODE (UCC) AND THE EU SECOND PAYMENT SERVICES DIRECTIVE (PSD2)

Introduction

A payment transaction is initiated by the order of the originator to the 'Originating (or originator's) Bank'. Where both end parties have their accounts in one bank, the transfer is in-house, and no further payment orders are required. Otherwise, in an interbank payment transaction, in the execution of the originator's payment order, the originating bank is to issue its own payment order either to the destination bank or to an intermediary bank. Figure 9 above, demonstrates the interaction between the participants of a payment transaction.

An 'Intermediary Bank' is needed whenever the originating bank and the 'Destination Bank' do not have a settlement link to facilitate the transfer of funds from one bank to another. Such a settlement link can be provided by either a correspondent relationship, under which one bank has an account with the other or through participation in a settlement system under which all participants settle on the books of a central counterparty, possibly the central bank. In a credit transfer, when no settlement link is available between the originating bank and the destination bank, the originating bank will instruct an intermediary bank, with which it has such a link, to make the payment. Where this intermediary bank does not have a settlement link with destination bank, it will instruct another intermediary bank to make a payment, until ultimately, there will be an intermediary bank having a settlement link both with the sender and the destination bank. An interbank credit transfer thus involves the originating bank and destination bank, and may further involve one or more intermediary banks.

Payment transactions are either debit or credit transfers. Where payer's instructions are communicated directly to the payer's bank, there is a credit transfer. Where payer's instructions are communicated to payer's bank indirectly, namely via payee and payee's bank, there is a debit transfer. Accordingly, in a credit transfer, the originator is the payer while the receiver is the payee. Conversely, in a debit transfer, the originator is the payee while the receiver is the payer. To that end, in discussing a debit transfer, it is common to focus not on the payer's instructions, but rather, on the payee's collection instructions initiated on the basis of the payer's authorization.

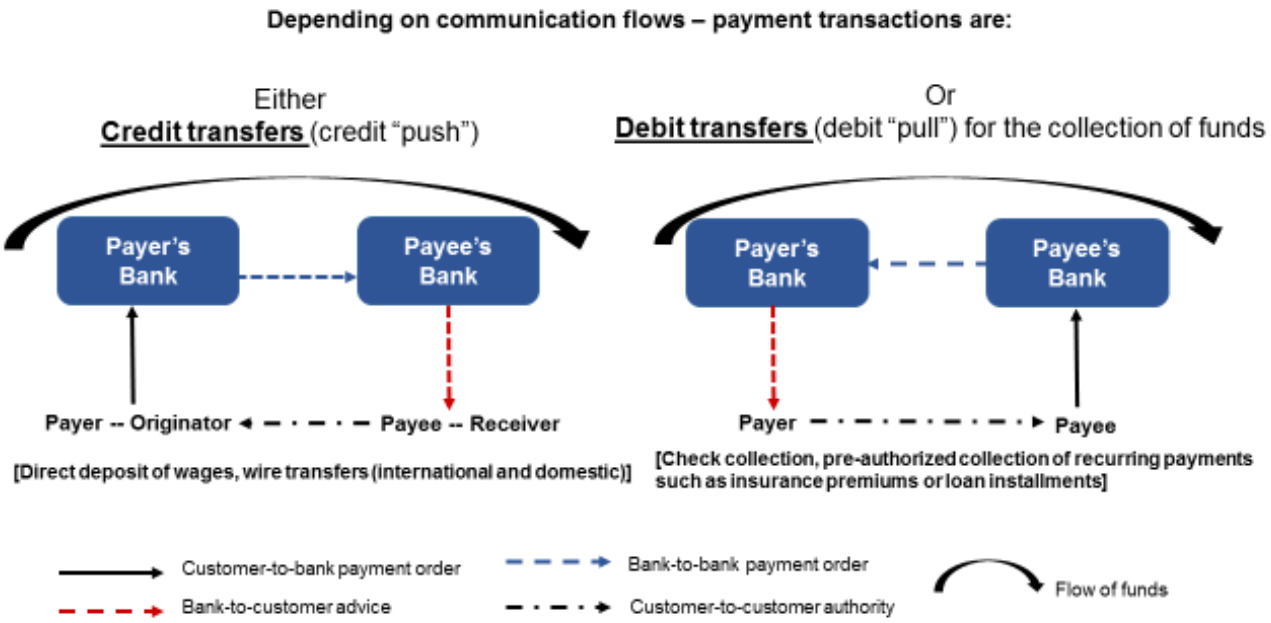
In a credit transfer, the payer's instructions that are communicated to the payer's bank push funds to the payee. In a debit transfer, the payee's communication to the payee's bank pulls or draws funds from the payer's account. Thus, as a matter of banking operation, a credit transfer commences with a debit to the payer's account and is completed with a credit posted to the payee's account. Conversely, a debit transfer may commence with a credit (albeit provisional) posted to the payee's account and is completed with a debit to the payer's account. The banking process in a debit transfer is thus subject to reversal (e.g. where there are insufficient funds in the account of the receiver-payer-debtor). From this perspective, being irreversible, the credit transfer is safer not only to the payee but to the payment system as a whole.

So far as their itinerary is concerned, it is thus the payer's instructions to the payer's bank that initiate the banking process in a credit transfer while it is the payee's instruction to the payee's bank that initiate the banking operation in a debit transfer. Stated otherwise, an opposite role in the communication is assumed by each end party, payer and payee, in each payment application. Accordingly, the payer is the originator in a credit transfer and the destination party (receiver) in a debit transfer, while the payee is the originator in a debit transfer and the destination party (receiver) in a credit transfer.

The two end participants to a payment transaction are the originator and receiver. In a credit transfer, the originator is the payer and the receiver is the payee or beneficiary. Conversely, in a debit transfer, the payee is the originator, and the payer is the receiver. Communication flow is always from the originator to the receiver, namely, from the payer to the payee/beneficiary in a credit transfer, and vice versa (from the payee/beneficiary to the payer) in a debit transfer. For its part, the payment or funds flow is always from the payer to the payee; that is, it is from the originator to the receiver in a credit transfer, and from the receiver

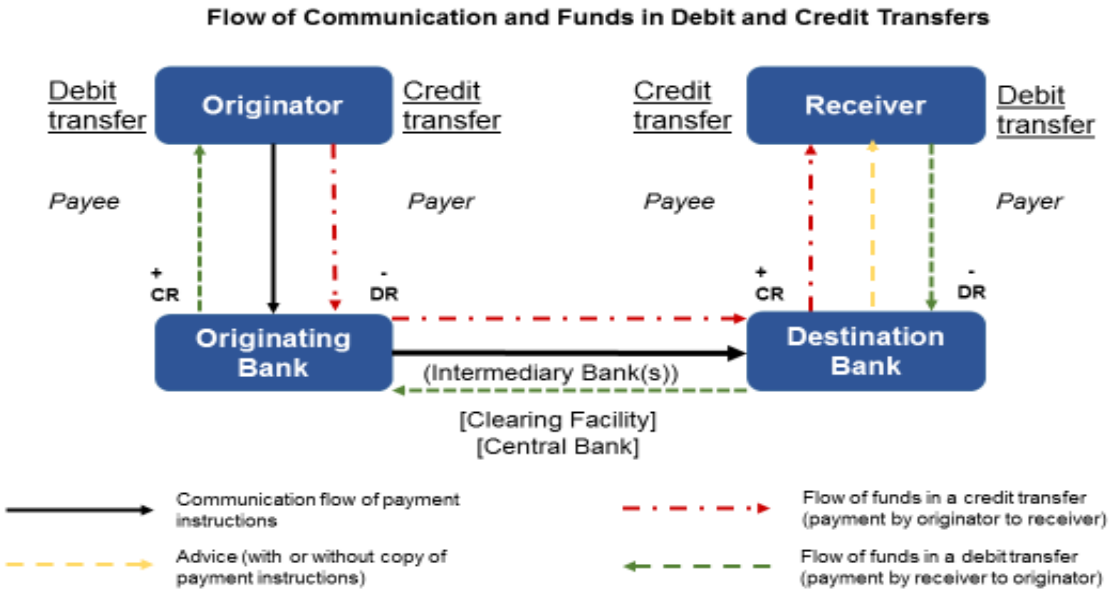
to the originator in a debit transfer. Stated otherwise, the payment and communication flows are in the same direction in credit transfers, and in opposite directions in a debit transfer. Either way, the banks of the originator and receiver are respectively, the originating and destination banks. As demonstrated in Figure 10, in a credit transfer, the originating bank is that of the payer and the destination bank is that of the payee; conversely, in a debit transfer, the originating bank is that of the payee while the destination bank is that of the payer.

Figure 10 Credit and Debit Transfers



The opposing roles of the originator and receiver in the payment transaction depending on whether it is a credit or debit transfer is highlighted in the following illustration.

Figure 11 Flow of communication and funds in debit and credit transfers



Scope

The transaction covered by UCC Art. 4A is a non-consumer[108] credit transfer, referred to as a funds transfer.[109] It consists of a series of transactions, beginning with the originator's payment order, made to make payments to the beneficiary of the order.[110] A 'payment order' means an instruction of a sender to a receiving bank, transmitted orally, in writing, or electronically (whether online or offline), to pay, or cause another bank to pay, a fixed or determinable amount of money to a beneficiary.[111]

Accordingly, for each payment order, the parties are the sender and the receiving bank. In connection with an interbank transfer, other than solely between accounts in correspondent banks, the parties to a funds transfer are the originator, the originator's bank, one or more intermediary banks, the beneficiary's bank and the beneficiary.

The scope of PSD2 is stated in Art. 2(1) of the Directive as to 'apply to payment services provided within the Union,', both national and cross-border. Payment services are defined in Art. 4(3) to mean business activities listed in Annex I.[112] Entities that provide such services to customers, each of whom is a 'payment service user' being either a payer or payee,[113] are 'payment service providers', or PSPs. One such PSP is the 'account servicing payment service provider' (ASPSP), which is a payment service provider providing and maintaining a payment account for a payer.[114] In principle, PSD2 concerns 'only contractual obligations and responsibilities between the payment service user and the [PSP].'[115]

In the footsteps of the original PSD,[116] payment services listed in Annex I[117] are cash deposits and withdrawals in and from payment accounts;[118] the execution of payment transactions[119] in funds[120] (including electronic money)[121] held either on deposit in a payment account or covered by a credit line; execution of direct debits;[122] execution of payment transactions through a payment card or a similar device;[123] execution

---

[108] More specifically, UCC Section 4A-108 excludes "a funds transfer any part of which is governed by the Electronic Fund Transfer Act of 1978 (Title XX, Public Law 95-630, 92 Stat. 3728, 15 U.S.C. § 1693 et seq.) as amended from time to time."

[109] UCC Sections 4A-104 and -108. The MLICT calls the transaction (in Art. 2(a)) a "credit transfer".

[110] UCC Section 4A-104(a). Pertinent terms are defined in Sections 4A-103 to 105.

[111] UCC Section 4A-103(a)(1).

[112] PSD2 Art. 4(3).

[113] See definition in PSD2 Art. 4(10) in conjunction with PSD2 Arts. 4(8) and (9), defining '"payer" and "payee". *Ibid* Art. 4.

[114] PSD2 Art. 4(17).

[115] *Ibid* preamble, paragraph 87. PSD2 preamble, paragraph 87 further recognizes that the allocation of responsibilities and losses between PSPs and "their intermediaries, such as processors" is a matter of contract. Id.

[116] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC, 2007 O.J. (L 319) 1.

[117] The list is however quite disorganized and repetitive; for example, three items (card payments, direct debits, and credit transfers) are enumerated separately according to whether they are used in connection with a "payment account" or credit line.

[118] Payment account is defined as 'an account held in the name of one or more payment service users which is used for the execution of payment transactions'. *Ibid* Art. 4(12). The Proposal required the account to be used "exclusively" for the execution of payment transactions, which was unnecessarily restrictive.

[119] Payment transaction is defined as 'an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.' PSD2, supra n 44, Art. 4(5).

[120] Funds are defined as 'banknotes and coins, scriptural money and electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC.' *Ibid* Art. 4(25).

[121] Electronic money is defined as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions…and which is accepted by a natural or legal person other than the electronic money issuer." Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC, 2009 O.J. (L. 267) 7, 11 (16 September 2009).

[122] 'Direct debit' is defined as 'a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.' PSD2, Art. 4(23). The Preamble addresses the mechanics of a direct debit. *Ibid* preamble, paragraph 76.

[123] 'Payment card' is not defined. However, the Preamble addresses 'the use of a card or card-based payment instrument.' *Ibid* preamble, paragraph 68.

of credit transfers (including standing orders); execution of direct debits (including one-off direct debits); issuing of payment instruments[124] and/or acquiring payment transactions;[125] as well as money remittance services in funds accepted for the sole purpose of carrying out the payment transaction.[126] Under the original PSD, the concluding item in the Annex was the '[e]xecution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.' PSD2 deleted this item but added payment initiation services and account information services to Annex I, which will be further discussed below.

In the terminology of PSD2, the originator under UCC Art. 4A is the payer; the beneficiary under UCC Art. 4A is the payee; the originator's bank under UCC Art. 4A is PSD2 payer's payment service provider; and the beneficiary's bank under UCC Art. 4A is the PSD2 payee's payment service provider.

Two pieces of legislation from developed countries, one from each side of the Atlantic, are to be presented with the view of assessing their contribution to the reduction or elimination of the legal risk in credit transfers. The first is Art. 4A of the Uniform Commercial Code (UCC) in the United States, whose terminology and conceptual framework was followed by UNCITRAL in drafting the MLICT. The other is the Second Payment Services Directive (PSD2) of the European Union.

PSD2 is broader than UCC Art. 4A in several respects. In addition to governing rights and remedies in a credit transfer, as is the case in UCC Art. 4A, PSD2 also regulates non-bank payment service providers, as well as sets up a licensing regime applicable to them. It also deals with the transparency of conditions and information requirements for payment services. Specifically, PSD2 Title III which deals with 'Transparency of conditions and information requirements for payment services' in Arts. 38-60, applies to single payment transactions, framework contracts and payment transactions covered by them – in each case where the payment service user is a consumer.[127] Corresponding provisions in the United States appear in Regulation E.

Unlike the UCC Art. 4A, PSD2 does not exclude funds transfers over consumer electronic payment systems. Furthermore, in clear departure from Art. 4A, PSD2 is not limited to credit transfers and also covers debit transfers. On the other hand, PSD2 substantive provisions seem to be geared towards consumer electronic funds transfers, and overall, can easily be contracted out in relation to business payments. As well, PSD2 addresses only the position of the end parties and, unlike UCC Art. 4A, does not deal with the interbank domain. Finally, in terms of substantive law provided for credit transfers, UCC Art. 4A is by far more detailed and comprehensive. The substantive provisions in relation to payment transactions, particularly credit transfers, are the subject of the ensuing discussion.

PSD2 is complemented by Regulation (EU) 2015/751 'lay[ing] down uniform technical and business requirements for card-based payment transactions carried out within the Union, where both the payer's payment service provider and the payee's payment service provider are located therein.' Particularly, this regulation sets caps on interchange fees for card-based transactions. Art. 2(10) of the Regulation defines 'interchange fee' to mean 'a fee paid for each transaction directly or indirectly (i.e., through a third party)

[124] 'Payment instrument' is defined as 'a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order.' Id. Art. 4(14). Payment order is defined as 'an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction.' Id. Art. 4(13). 'Issuing of payment instruments' is defined as 'a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions.' Id. Art. 4(45).

[125] 'Acquiring of payment transactions' is defined as 'a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.' Id. Art. 4(44).

[126] 'Money remittance' is defined as 'a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.' Id. Art. 4(22).

[127] PSD2, Art. 38(1)

between the issuer and the acquirer involved in a card-based payment transaction.' This Regulation, as well as its subject matter, are not addressed in this Guide.

Legal risks addressed by UCC Art. 4A and PSD2 are discussed below by reference to 12 subjects: scope, the payment order and its acceptance or rejection, timely cancellation and automatic withdrawal of an (unexecuted) payment order, sender's payment obligation and its excuse under money-back guarantee upon non-completion of a credit transfer, sender's payment, sender's liability, fraudulent and mistaken payment orders, completion of credit transfer and discharge of underlying debt, liability for consequential losses by a receiving bank, restitution upon erroneous completion of credit transfer, third-party intermediaries, and law applicable: variations and cross-border- international setting.

The payment order and its acceptance or rejection

Under UCC Section 4A-103(a)(1), a payment order may be transmitted orally, electronically, or in writing. An interbank payment order may be transmitted over a funds-transfer system, that is, a communication network of a clearing house or another association of banks.[128] The domestic large-value transfer system for each country, such as CHIPS and Fedwire in the U.S., as well as the International Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, are such funds transfer systems. In the funds transfer, each payment order is a request by the sender to the receiving bank, which can be accepted or rejected. A payment order does not create an agency or mandate. Nor is it tantamount to the assignment of funds; rather, acceptance by a receiving bank of a sender's payment order generates a contract *sui generis* that does not fall into any established relationship. A receiving bank is neither an agent (of the sender, beneficiary or of any other participant), nor an assignee (of the originator's funds at the originator's bank). Acceptance inures solely to the benefit of an immediate party in private. Thus, acceptance by a receiving bank other than the beneficiary's bank inures to the benefit of the sender; acceptance by the beneficiary's bank inures to the benefit of the beneficiary.[129]

Acceptance of a payment order by the beneficiary's bank is either by paying (or advising) the beneficiary or, where the beneficiary has an account at the beneficiary's bank, by obtaining cover for such a payment.[130]

Acceptance by a receiving bank other than the beneficiary's bank is by the execution of the payment order – that is, by the issue of a corresponding payment order, intended to carry out the one received by the bank.[131] The executing bank must issue a payment order that strictly conforms to that received by it with respect to the amount, the ultimate destination of the funds, and the identity of any specifically designated intermediary bank. Otherwise, the executing bank's duties as to speed, the means of communication, the use of a funds-transfer system, and the selection of an intermediary bank, where none are designated by the sender, are to be carried out with reasonable care and skill.[132] Nothing short of 'execution' serves as acceptance by a receiving bank other than that of the beneficiary. Stated otherwise, giving notice of acceptance, obtaining cover for the payment order or incurring an obligation to accept, will not serve as acceptance by a non-beneficiary's bank.[133] An effective obligation to accept must be solely by express agreement but by itself is not acceptance.[134]

[128] UCC Section 4A-105(a)(5).

[129] See in general UCC Section 4A-212 (any official comment) as well as Section 4A-209 official comment 1.

[130] Under Art. 9(1) of the MLICT, acceptance by the beneficiary's bank is constituted also (i) upon receipt of the payment order (but only if so agreed to by the sender) or (ii) by giving notice to the sender.

[131] UCC Sections 4A-209 and 301.

[132] UCC Section 4A-302.

[133] In this respect, the MLICT is different. Under Art. 7, acceptance by a receiving bank other than the beneficiary's bank may occur not only by execution, but also (i) upon receipt of the payment order by the receiving bank (but only if so agreed), (ii) by giving notice of acceptance to the sender, (iii) by debiting the sender's account or (iv) automatically after the expiry of the rejection period (usually on the second banking day following the receipt of the payment order), provided no notice of rejection had been given (but only where sender's funds are available and sender information in the payment order is adequate).

[134] UCC Section 4A-212.

Notice of rejection is required to avoid liability for interest and may preclude acceptance by a beneficiary's bank holding adequate funds as cover.[135] Otherwise, there is no acceptance by inaction or mere passage of time. Suspension of payment by a receiving bank is tantamount to rejection by the operation of the law. In general, the occurrence of either acceptance or rejection is irreversible.[136] No duty is fastened on a bank that has neither accepted nor rejected a payment order.[137]

PSD2 Art. 78(1) provides that '[t]he payer's account shall not be debited before receipt of the payment order.' To that end, it identifies the time of receipt with when the payment order is received by the payer's [PSP]. It goes on to state that if the point of time of receipt is not on a business day for the payer's payment service provider, a receipt is deemed to occur on the following business day. Additionally, the payer's service provider may establish a cut-off time near the end of the business day beyond which receipt will be deemed to occur the following business day. As well, and on this point in the footsteps of UCC Section 4A -106, the payer's service provider may establish a cut-off time, though only near the end of the business day, beyond which receipt will be deemed to occur the following business day. The Payment Services Directive (PSD) does not address issues relating to an interbank payment order.

PSD2 Art. 79 governs refusal of payment orders. Art. 79(1) fastens on the PSP that refuses to execute a payment order a duty to advise the user of the refusal and, if possible, the reason for it and the procedure for correction. Per the framework contract, the user may be charged for the notification of an objectively justified refusal.[138] On its part, the right to refuse is not entirely discretionary to the PSP. According to PSD2 Art. 79(2), and 'irrespective of whether the payment order is initiated by a payer … or through the payee,' namely, both in credit and debit transfer,[139] '[w]here all of the conditions set out in the payer's framework contract are met, the payer's [ASPSP] shall not refuse to execute an authorized payment order.'[140]

The position under UCC Art. 4A of an originator's bank that rejects a payment order is more favourable. More specifically, under UCC Section 4A-212, '[i]f a receiving bank fails to accept a payment order that it is obliged by express agreement to accept, the bank is liable for breach of the agreement to the extent provided in the agreement or in this Article [4A].' Otherwise, and 'except as provided in this Article or by express agreement,' a receiving bank 'does not … have any duty to accept a payment order or, before acceptance, to take any action or refrain from taking action, with respect to a payment order …'. Thus, while as under PSD2, liability is based on contract,[141] the scope of liability is stated to be narrower under the UCC. Stated otherwise, unlike UCC Section 4A-212, PSD2 Art.79 does not restrict liability by reference to its own provisions or the express agreement of the parties. In fact, liability provided under Art. 4A is only for the failure to advise of rejection of a payment order, which is only for lost interest.[142]

---

[135] See UCC Section 4A-209(b)(3).

[136] Rejection of payment order is governed by UCC Section 4A-211.

[137] Conversely, the MLIC imposes on a receiving bank that has not rejected a payment order, assistance, inquiry and notice obligations, even in the absence of acceptance on its parts. See e.g. Arts. 8, 10 and 13.

[138] *Ibid*. This is in fact enumerated as one of the "information obligations" for which the payment service provider may charge the payment service user. Id. Art. 62(1). Notification is to be made "in an agreed manner at the earliest opportunity." Id. Art. 79(1). This duty is to be complied with "unless prohibited by other relevant Union or national law." Id.

[139] PSD2 Art. 79(2). Also in the absence of a prohibition by Union or national law.

[140] *Ibid*. ASPSPs are discussed below in #11. According to the PSD2 preamble, paragraph 77, "[u]sers should be able to rely on the proper execution of a complete and valid payment order if the payment service provider has no contractual or statutory ground for refusal. If the payment service provider refuses a payment order, the refusal and the reason for the refusal should be communicated to the payment service user at the earliest opportunity, subject to the requirements of Union and national law. Where the framework contract provides that the payment service provider may charge a fee for refusal, such a fee should be objectively justified and should be kept as low as possible."

[141] Though unlike UCC Section 4A-212, PSD2 lacks the emphasis on "express" agreement, so even on this point it is less favourable to the payer's payment service provider (that is, the originator's bank).

[142] Under UCC Section 4A-210(b), specifically referred to (together with UCC Section 4A-209(b)(3) that does not apply to the originators bank) in Official Comment to UCC Section 4A-212.

Timely cancellation and automatic withdrawal of an (unexecuted) payment order

Under UCC Art.4A, a payment order is cancelled by operation of law if it remains unaccepted for five days, as well as where the receiving bank knows of the sender's death or legal incapacity before acceptance. Otherwise, a payment order can be cancelled or amended by means of communication of the sender to the sender's receiving bank. Cancellation or amendment can be made by the sender unilaterally up to the time of acceptance by that receiving bank. After acceptance, and in the absence of an agreement or a funds-transfer system rule to the contrary, cancellation or amendment requires the agreement of the receiving bank. Where a receiving bank other than that of the beneficiary agrees to the cancellation or amendment, a conforming cancellation or amendment must be issued by it to its own receiving bank.[143] The funds transfer is thus effectively aborted if the last receiving bank to receive a payment order is advised by its sender of the cancellation or amendment prior to the acceptance of the payment order by that receiving bank.

Where the receiving bank is the beneficiary's bank, post-acceptance cancellation or amendment can be made only with respect to an unauthorized or mistaken funds transfer. As with respect to any post-acceptance cancellation or amendment, agreement of the receiving bank, in this case, the beneficiary's bank, is required. Unless otherwise provided by an agreement or funds-transfer system rule, the sender is liable to a receiving bank for any loss incurred by that bank in a post-acceptance cancellation (or amendment) or attempted cancellation (or amendment).[144]

Injunction and creditor process by the originator's creditors can prevent the originator's bank from initiating a funds transfer. Likewise, an injunction and creditor process by the beneficiary's creditors can prevent the beneficiary from receiving the benefit of payment once the funds transfer has been completed. A funds transfer cannot, however, be intercepted by third parties between acceptance by the originator's bank and by the beneficiary's bank.[145]

PSD2 Art.80(1) precludes the revocation of a payment order 'once it has been received by the payer's [PSP].' For credit transfers, this is a noteworthy departure from UCC. Art. 4A, where revocation is permitted until execution by the payer's service provider.[146] However, the framework governing the ability of parties to provide for revocability is unclear. Thus, under PSD2 Art. 61(1), irrevocability may be contracted out only '[w]here the payment service user is not a consumer.' At the same time, under PSD2 Art. 80(5), and irrespective as to whether the payment transaction is a consumer or business transaction, revocability beyond points of time specified in PSD2 Art. 80 may be a matter of an agreement between the payment service user and his or her PSP, for which the PSP may charge the payment service user if so agreed in their framework contract.[147]

Aside from an agreement, as above, for a payment transaction initiated either by a PISP or by or through the payee, revocability is denied even prior to receipt under PSD2 Art. 80(1). Thus, according to PSD2 Art. 80(2), for such a payment transaction, 'the payer shall not revoke the payment order after giving consent to the [PISP] to initiate the payment transaction or after giving consent to execute the payment transaction to the payee.'

However, under PSD2 Art. 80(4), revocability is available for payment orders instructing payment in the future, though 'at the latest by the end of the business day preceding the agreed day.' For 'a direct debit[148] and without prejudice to refund rights' the same rule is specifically provided in Art. 80(3).

---

[143] UCC Section 4A-211.

[144] *Ibid.*

[145] UCC Sections 4A-502 and 4A-503.

[146] UCC Section 4A-211.

[147] This is in fact enumerated in Art. 62(1) as one of the "corrective and preventive measures" for which the payment service provider may charge the payment service user. Id. Art. 62(1).

[148] A direct debit is a debit transfer carried out as part of a 'payment service', namely, a 'business activity listed in Annex I.' Id. Art. 4(3). A "debit transfer" is defined as "a payment transaction…initiated by the payee on the basis of the consent given by the payer to the

Sender's payment obligation and its excuse under "money-back guarantee" upon non-completion of a credit transfer

Under UCC Section 4A-402, the acceptance of a payment order by a receiving bank obliges the sender to pay the amount of the order. However, under what came to be known as the money-back guarantee rule,[149] payment by the sender is excused or can be refunded to it, where the funds transfer is not completed. Nonetheless, an originator that selected a failed intermediary bank is responsible for the amount prepaid by the sender to that bank. Otherwise, where loss occurred at an intermediary bank, the effect of the money-back guarantee rule is to shift the risk of loss away from the originator and to place it on the sender to the insolvent bank, regardless of whether the loss was caused by a breach of duty.

Similarly, under PSD2 Art. 89(1), in principle, the payer's 'payment service provider shall … be liable to the payer for the correct execution of the payment transaction.' Effectively, the payer's PSP is discharged at the point of time in which 'the payee's [PSP] [timely] received the amount of the payment transaction…'.A payer's PSP in breach with its obligation, 'shall, without undue delay, refund to the payer the amount of the non-executed or defective payment transaction, and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.' Stated otherwise, the payer is entitled to a money-back guarantee from the payer's payment service provider in case funds do not reach the payee's payment service provider. Regardless of breach or defence to liability, in the case of non-execution of defective execution, and on request, the payer's payment service provider shall 'make immediate efforts to trace the payment transaction and notify the payee of the outcome.'

Sender's payment

Under UCC Section 4A-403, sender's payment is carried out usually by means of

- An interbank final settlement over a funds-transfer system;
- A credit by the sending bank to the receiving bank's account, in which case payment occurs at the midnight of the day on which the credit is withdraw-able and the receiving bank learns of this fact unless credit was withdrawn earlier, in which case payment occurred at the time of withdrawal;[150] or
- A debit by the receiving bank to the sender's account, provided funds are actually available in the account.

Where the receiving bank is that of the beneficiary, payment through a debit to the sender's account containing adequate cover, in fact, even by means of the availability of cover for a debit in such an account, will constitute acceptance only at the opening of the next funds-transfer system day, provided the payment order was not rejected until one hour thereafter.[151]

PSD2 Art. 81 deals with the amount of a payment transaction. Similarly to UCC Art. 4A-302 (d),[152] its basic principle under PSD2 Art. 81(1) is that the full amount instructed is to be transferred so that no charges are to be deducted by the payer's, as well as the payee's, service provider and by any intermediary. Fees are to

payee, to the payee's payment service provider or to the payer's own payment service provider." Id. Art. 4(23). This is distinguishable from an isolated debit transfer.

[149] See UCC Section 4A-402 Official Comment 2.

[150] Conversely, under MLICT Art. 6(b) sending bank's payment of a payment order by crediting the receiving bank's account occurs when this credit is used or, if not used, on the banking day following the day on which the credit is available for use to the knowledge of the receiving bank (rather than at midnight of the day on which the credit is withdraw-able as under Art. 4A).

[151] UCC Section 4A-209(b) (3). Contrary, under MLICT Art. 9(1)(c), acceptance of the beneficiary's bank by means of debiting the sender's account occurs when the beneficiary's bank actually debits the account. Under MLICT Art. 9(1)(h), automatic acceptance by the mere availability of sender's funds (without actually debiting the sender's account) takes place on the second banking day following the receipt of the payment order (containing sufficient information to identify the sender) unless notice of rejection was given prior to that.

[152] UCC Section 4A-302(d) precludes the receiving bank, "[u]nless instructed by the sender", to obtain or instruct a subsequent receiving bank to obtain charges and expenses by deducting them from the sender's payment order. Cf. also UCC Section 4A-404(c).

be charged to the account as such and not be deducted from the amount transferred. Thus, under PSD2 Art. 81(2), an agreed charge may be debited separately to the payee's account by his or her payment service provider, rather than made as a deduction to the amount credited. Per PSD2 Art. 81(3), it is up to the service provider of the party initiating the payment transaction to ensure that the payee receives the full amount of the payment transaction.

PSD2 does not address specifically the sender's payment, including interbank one. However, PSD2 Art. 83 effectively addresses execution of the payment transaction by reference to either the receipt of funds by the payee's payment service provider in the form of a credit to its account, or to crediting the payee's account by its payment service provider. In this context, it is not clear why receipt of funds by the payee's service provider is necessarily limited to the situation where funds are so received by means of credit posted to the account of the payee's payment service provider. Certainly, as discussed, per UCC Section 4A-403, funds can be received by other ways as well, including debit to the account of the payer's payment service provider.

Sender's liability

Certainly, one is bound by a payment order he or she transmitted. As well, under UCC Art. 4A, to bind a person as a sender, the payment order must be an authorized payment order for which this person is bound under the law of agency. Also, unless proven that the payment order 'was not caused directly or indirectly by a person' under its control, a customer is bound by any payment order whose authenticity was verified by the bank according to a commercially reasonable security procedure agreed upon between the customer and the bank.[153]

Under UCC Section 4A-204, a receiving bank accepting a payment order issued in the name of its customer that is neither authorized nor effectively verified is required to refund any payment made by the customer for that payment order. The receiving bank is further liable to pay interest for the refundable amount. However, liability to pay interest is excused upon the customer's failure to exercise ordinary care to determine lack of authority and to notify the bank with respect to it 'within a reasonable time not exceeding 90 days after the date the customer received notification from the bank …'. Furthermore, under UCC Section 4A-505, having failed to challenge a debit for an unauthorized or unverified payment order posted to the customer's account within one year of receipt of notification from the bank, the customer is precluded altogether from contesting it.

Arts. 64-77 in Chapter 2 of PSD2 govern the authorization of payment transactions. The provisions cover authorization in general and electronic authorization in particular, the onus of proof, liability for losses, as well as reversal of authorized debit transfers.

Authorization in the form of consent is to be given for the execution of a payment transaction. PSD2 Art. 64 treats authorization only in terms of the payer's consent, which is also required for debit-pull withdrawals by the payee from the payer's account. No reference is made to the payee's authorization given to the payee's PSP as to carrying a debit transfer out of the payer's account.

Authorization in the form of payer's consent may be given under Art. 64 'prior to or, if agreed between the payer and the [PSP], after the execution of the payment transaction' and in the form as well under the procedure agreed between them.[154] Consent to execute a payment transaction may also be given via the payee or the PSP. In the absence of [such] consent, a payment transaction shall be considered to be unauthorized.[155]

[153] See UCC Sections 4A-201 to 4A-203. Under Section 4A-201, "[a] security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, call-back procedures, or similar security devices. Comparison of a signature of a payment order with an authorized specimen signature of the customer is not by itself a security procedure."

[154] PSD2, Art. 64(1) and (2)

[155] *Ibid*. Proviso to Article 64(2)

Consent under PSD2 is not necessarily required to be explicit.[156] However, the reference to an agreement as well as a procedure weakens the possibility of implied authority and may be read to eliminate altogether the possibility of apparent authority,[157] as when a cardholder voluntarily delivered the card and advised the associated code to a friend or relative.[158] In fact, as discussed below, under Art. 65-67, consent to be given to a PISP, ASPSP and AISP is required to be explicit.

Under PSD2 Art. 64(3), consent 'may be withdrawn by the payer at any time, but no later than at the moment of irrevocability' of the payment order under Art. 80. Also, withdraw-able is '[c]onsent to execute a series of payment transactions,' in which case 'any future payment transaction shall be considered as unauthorised.'[159]

According to PSD2 Art. 65, at the request of a PSP card issuer, the ASPSP shall immediately advise it as to the availability of funds on the payer's payment account 'for the execution of a card-based payment transaction', but only where the payer has given explicit consent to the ASPSP to respond to such requests from that PSP. Confirmation is required to be laconic; the ASPS ought not to disclose the account balance and is not allowed to block funds. For its part, the PSP may not store or use the response other than for the execution of the card-based payment transaction.[160]

Under PSD2 Art. 66(1), Member States are required to 'ensure that a payer has the right to make use of a [PISP]' but only where the payment account is accessible online. For a payment to be authorized, the payer's explicit consent may be given to a PISP.[161] Under PSD2 Art. 66(3), a PISP shall not hold the payer's funds in connection with the provision of the PIS; prevent unauthorized access to the personalized security credentials[162] of, and other information about, the payment service user; identify itself towards the payer's ASPS and communicate with it and the parties to the payment transaction in a secure way; not store sensitive payment data of the payment service user and not request from him data other than those necessary to provide the payment initiation service; not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer; and not modify any feature of the transaction. For its part, under Art. 66(4), the ASPS is required to communicate securely with the PISP, promptly provide information to it, and 'treat payment orders transmitted through the services of a [PISP] without any discrimination…'[163]

The payment service user's right to make use of an AISP for a payment account accessible online is provided for by PSD2 Art. 67(1). Under Art. 67(2), the AISP is required to provide services only where based on the payment service user's explicit consent; prevent unauthorized access to the personalised security credentials of the payment service user; identify itself towards the payer's ASPS and communicate with it in a secure way; access only the information from designated payment accounts and associated payment transactions; and not use, access or store any data for purposes other than for performing the AIS explicitly requested by the payment service user. For its part, the ASPS, under PSD2 Art. 67(3), is obligated to communicate securely with the AISPS and treat data requests involving it without any discrimination.[164]

---

[156] This is in departure from the Lisbon Programme Proposal, supra n 68, Art. 41, under which '[c]onsent shall consist in an explicit authorization for the payment service provider to effect a payment transaction or a series of transactions.'

[157] As a matter of agency law, authority can be actual or apparent ("Agency", Black's Law Dictionary (10th ed. 2014)). Actual authority may be express or implied ("Authority", Black's Law Dictionary (10th ed. 2014)).

[158] In this case, liability may nevertheless be fastened on the cardholder. PSD2, Art. 74(1).

[159] The withdrawal of consent to a single future payment transaction (rather than to a series of them) falls under the previous sentence.

[160] Note that per PSD2 Art. 65(6), 'Article [65] does not apply to payment transactions initiated through card-based payment instruments on which electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC is stored.'

[161] PSD2 Art. 64(2); see also id. Art. 80(2) ('[w]here the payment transaction is initiated by a [PISP]…, the payer shall not revoke the payment order after giving consent to the [PISP] to initiate the payment transaction…').

[162] 'Personalised security credentials' are defined as 'personalised features provided by the payment service provider to a payment service user for the purposes of authentication.' Id. Art. 4(31).

[163] See also PSD2 Art. 68(5) (discussing denial 'for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by…that [PISP]').

[164] See also PSD2 Art. 68(5) (discussing denial "for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by…that [PISP]").

The Directive contemplates authorization to be given either in an electronic form or otherwise.[165] An electronic authorization is referred to as authorization given by means of a payment instrument. Important aspects of such authorization are governed by Art. 68-70. Payment instrument is defined in Art. 4(14) as 'a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used [by the payment service user] in order to initiate a payment order.' A card used with or without a personal code will satisfy this definition. Moreover, any agreed-upon security procedure will be a payment instrument.

Limits to the ability to initiate a payment transaction by means of a payment instrument are provided for in Art. 68. Thus, under Art. 68(1), where a specific payment instrument is used for the purposes of giving consent, an authorization may be given within agreed 'spending limits for payment transactions executed through that payment instrument.' As well, according to Art. 68(2), under the 'framework contract, the [PSP] may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument' or similar reasons. Similarly, under Art. 68(5), '[a]n [ASPSP] may deny an [AISP] or a [PISP] access to a payment account,' albeit only 'for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that [AISP] or that [PISP], including the unauthorised or fraudulent initiation of a payment transaction.' In such cases, the ASPSP shall promptly inform the payer and, per Art. 68(6), report the incident to the authorities.

Art. 69 and 70 govern reciprocal obligations of payment service user and provider in relation to payment instruments. Thus, under Art. 69, the payment service user is required to 'use the payment instrument in accordance with the terms governing the issue and use of the payment instrument,' and in particular, to take all reasonable steps to keep safe the personalized security payment instrument. The user is further required to notify the PSP 'without undue delay upon becoming aware of loss, theft or misappropriation or unauthorised use of the payment instrument.'[166]

In turn, the PSP issuing a payment instrument is required under PSD2 Art. 70(1):

(a) To make sure that the personalized security credentials of the payment instrument are not accessible to third parties;

(b) To refrain from sending an unsolicited payment instrument other than as a replacement to an existing one;

(c) To ensure that appropriate means are available at all times to enable the payment service user to make required notifications, for example, upon the loss, theft, or misappropriation of the payment instrument;[167]

(d) To provide the payment service user with an option to make such a notification free of charge[168] and to charge, if at all, only replacement costs directly attributed to the payment instrument;

(e) To prevent the use of the payment instrument once such notification has been made.

[165] Stated otherwise, a payment transaction falling under the Directive needs not be electronic from end to end; rather, authorization can be given in writing. In fact, even an oral authorization is not precluded.

[166] This requirement does not apply to 'payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time,' and which 'does not allow its blocking or prevention of its further use.' PSD2 Art. 63(1)(a).

[167] This requirement does not apply to 'payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time," and which "does not allow its blocking or prevention of its further use.' PSD2 Art. 63(1)(a).

[168] This requirement does not apply to 'payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time,' and which 'does not allow its blocking or prevention of its further use.' PSD2 Art. 63(1)(a).

PSD2 Art. 70(2) allocates to the PSP 'the risk of sending a payment instrument or any personalized security credentials relating to it to the payment service user.' No reciprocal broad general duties of care to prevent and detect unauthorized use are fastened on the payment service user and provider.

Under PSD2 Art. 72, where a purported payer denies authorization for a payment transaction as debited to his or her account, it is for his or her payment service provider 'to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.' However, 'authenticated'" is defined by reference to the verification of the authorization by means of a payment instrument.[169] The provision goes on to state that 'the use of a payment instrument recorded by the [PSP], including the [PISP] as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorized by the payer or that the payer acted fraudulently or failed with intent or gross negligence[170] to fulfil one or more of the obligations under Art. 69.'[171] Stated otherwise, evidence as to the use of a payment instrument recorded by the service provider is an important element in meeting the required standard of proof for fastening civil liability for authorized use; yet, standing on its own, such evidence creates neither an irrefutable[172] nor even a rebuttable presumption that reverses the onus of proof as to whether use was authorized.[173] Rather, some corroboration is required.[174]

Art. 71, 73, and 74 govern the allocation of losses for unauthorized payments.

First, under Art. 71(1), unless the PSP failed to make disclosures required under Title III of the Directive dealing with transparency and information requirements for payment services, the payment service user is entitled to obtain rectification from it only if the user notifies the provider 'without undue delay on becoming aware of any such transaction giving rise to a claim…and no later than 13 months after the debit date.'[175] The same applies '[w]here a [PISP] is involved.'[176] Under Art. 73, whether or not the payment transaction was initiated through a PISP, refund by the payer's PSP to the payer is to be made immediately, for the amount of the unauthorized payment transaction. 'Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and his [PSP] or the contract concluded between the payer and the payment initiation service provider if applicable.'[177] Presumably, such

---

[169] "Authentication" is defined as a "procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials." PSD2, Art. 4(29). There is no requirement comparable to UCC Section 4A-202(b) for a 'security procedure', which is 'a commercially reasonable method of providing security against unauthorized payment orders.' UCC Section 4A-202(b) (Am. Law Inst. & Unif. Law Comm'n 2012).

[170] According to the PSD2 preamble, paragraph 72: '[i]n order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases.'

[171] PSD2 Art. 72(2). Per Art. 61(1), 'where the payment service user is not a consumer, the payment service user and the [PSP] may agree that…Article[] 72…[does] not apply "in whole or in part." Id. Art. 61(1). Also, under Art. 63(1)(b), in connection with low-value payments, Art. 72 does not apply "if the payment instrument is used anonymously or the [PSP] is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised.' Id. Art. 63(1)(b), 72.

[172] Judd v. Citibank, 107 Misc. 2d 526, 529 (Civ. Ct. 1980) (stating that the court was "not prepared to go so far as to rule that where a credible witness is faced with the adverse 'testimony' of a machine, he is as a matter of law faced also with an un-meetable burden of proof").

[173] Compare PSD2 Art. 72(2), with UCC Section 4A-203.

[174] Such as lack of credibility or some support to user's version.

[175] The notification requirement is stated to apply also to a claim for incorrectly executed payment transactions governed by PSD2 Art. 89.

[176] PSD2 Art. 71(2) adds that the payment service user's rectification from the ASPSP is 'without prejudice to Art. 73(2) and Art. 89(1)', which is discussed further below.

[177] Under PSD2 Art. 63(1)(b), in connection with low-value payments, Art. 73 does not apply 'if the payment instrument is used anonymously or the [PSP] is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised.

loss will be also for wrongful dishonour for items that lacked cover due to the debit for the unauthorized payment.

Second, PSD2 Art. 74 provides for the liability of the payer for unauthorized payment transactions. Under Art. 61(1), the provision can be contracted out where the payment service user is not a consumer. Its rules can be set out – albeit not in the sequence they are provided in the article itself – as follows:

1. The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence.[178]

As recalled, under Art. 69, the payment service user is required to use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, and in particular, to take all reasonable steps to keep safe the personalized security payment instrument. However, not every breach of such a term results in an unlimited liability; rather, per the language of Art. 74(1), the failure to fulfil an obligation under Art. 69 must have been made 'with intent or gross negligence.' Arguably, however, unlimited liability for gross negligence may be fastened in cases that would have otherwise been treated as those of apparent authority - as for example, where the payment service user delivers the payment instrument to one considered by the payment service user to be a trusted agent who nevertheless betrays him or her. Other than in low-value payments, where the payment instrument does not allow its blocking or prevention of its further use, the payer is further required to notify the PSP 'without undue delay on becoming aware of the loss, theft or misappropriation or unauthorised use of the payment instrument.'[179]

2. A payer who has not acted fraudulently[180] is released from liability where:

   (a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment;[181]

   (b) the payer's PSP does not require 'strong customer authentication',[182] defined in Art. 4(30) to mean 'an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.' A PIN used in conjunction with a card will meet this standard, which is not the case for either a PIN or card alone. Under Art. 97(1), a PSP is required to apply strong customer authentication where the payer '(a) accesses its payment account online; (b) initiates an electronic payment transaction; (c) carries our any action through a remote channel which may imply a risk of payment fraud or other abuse.' For remote electronic payment transactions,[183] PSPs are required by Art. 97(2) to 'apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.' For their part, PSPs are to be mandated under Art. 97(3) to 'have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.' In

[178] Inasmuch as he did not 'allow…a payment order from [the] payment account' nor '[gave] a payment order' as required for a 'payer' under Art. 4(8), reference should have been in Art. 74 (and hence to all the rules set out below) to the 'purported payer' and not the 'payer.'

[179] PSD2 Art. 69(1)(b).

[180] Note that under the plain meaning of the provision, a payer who has acted with gross negligence is still protected under the prescribed circumstances.

[181] PSD2 Art. 74(1)(a).

[182] PSD2 Art. 74(2) (providing that '[w]here the payee or the [PSP] of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.').

[183] 'Remote payment transaction' is defined as 'a payment transaction initiated via internet or through a device that can be used for distance communication.' PSD2 Art. 4(6). There is no definition for 'electronic payment transaction.' Cf. reference to definitions elsewhere of 'electronic communications network' and 'electronic communications service' respectively under Art. 4(41) and (42) as well as of 'electronic money' in Art. 18(3).

turn, under Art. 97(5), PISPs and AISPs may 'rely on the authentication procedures provided by the [ASPSP] to the payment service user.'

(c) other than in connection with a payment instrument (for low-value transactions) which does not allow its blocking or prevention of its further use, after prompt notification, in accordance with Art. 69(1)(b), upon becoming aware of loss, theft or misappropriation of the payment instrument or its unauthorized use;[184] or

(d) the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, in breach of Art. 70(1)(c) (which does not apply to in low-value payments where the payment instrument does not allow its blocking or prevention of its further use).

3. The payer is released from liability where 'the loss was caused by acts or lack of action of an employee, agent or branch of a [PSP] or of an entity to which its activities were outsourced.'[185]

4. In other circumstances, 'the payer may be obliged to bear the losses relating to any unauthorized payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.'[186] Such could be the case where the failure to fulfil one or more of the obligations set out in Art. 69 was neither intentional nor with gross negligence as set out in Rule #1.

5. Where the payer has neither acted fraudulently nor intentionally failed to fulfil his or her obligations under Art. 69 (summarized in Rule #1 above), 'Member States may reduce the liability referred to in [Rules # 1 and # 4], taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.'[187]

Fraudulent and mistaken (albeit authorized) payment orders

A payment order must identify the beneficiary, as well as the beneficiary's bank. It may further identify an intermediary bank. A beneficiary is typically identified by name or account number. A bank may be identified by name or identification number. Misdescription, whether caused erroneously or fraudulently,[188] may lead to the diversion of funds to an unintended beneficiary.

According to UCC Section 4A-207(a), a payment order for a non-existent or unidentifiable beneficiary cannot be accepted by the beneficiary's bank.[189] Where a payment order identifies the beneficiary by name and number, the beneficiary's bank, acting without knowledge of any inconsistency between the name and number, may rely on the number. Where funds consequently reach an unintended beneficiary, the loss will fall on the originator (who remains liable to the intended beneficiary). However, a non-bank originator who was not advised of this risk may shift the loss to the originator's bank. Recovery from the person identified by the number who was not entitled to receive payment from the originator is available, to the extent allowed by the law of mistake and restitution.[190]

[184] Cf. Minskoff v. Am. Express Travel Related Servs. Co., 98 F.3d 703 (2d Cir. 1996) (holding that receipt of a statement reasonably putting the customer on notice that one or more fraudulent charges have been made precludes an argument based on lack of knowledge of these charges).

[185] PSD2 Art. 74(1)(b).

[186] Id. Art. 74(1).

[187] Id.

[188] A typical fraudulent design is outlined e.g. by Benjamin Geva, The Law of Electronic Funds Transfers (2018) at the beginning of §2.07[3].

[189] For a detailed discussion, see e.g. Geva, *Ibid* at §2.07[2].

[190] UCC Section 4A-207(b), (c) and (d).

Where a payment order identifies an intermediary or beneficiary's bank by number or name and number, the receiving bank acting without knowledge of any inconsistency may act either on the number or the name. The rules applicable to erroneous execution determine the allocation of loss.[191]

In an electronic environment, typical errors in the dispatch or contents of a payment order include the transmittal of a duplicate payment order, an increase in the amount of a payment order (for example, by the addition of zeros to the sum), or the instruction of payment to an unintended beneficiary (usually by erring in the account or identification number of the intended beneficiary). Art. 4A provides for the allocation of responsibility for such errors.

In principle, the sender is responsible for the contents of its own payment order. It is also responsible for a discrepancy arising in the course of the transmittal of a payment order through a third-party communication system (e.g. SWIFT). This means that such an intermediary system is deemed to be an agent of the sender who is bound by the contents of the payment order as sent to the receiving bank by that communication system.[192]

A sender can nevertheless shift to the receiving bank the loss arising from the transmittal of an erroneous payment order (whether by itself or by a communication system acting as its agent). Such is the case where the receiving bank has failed to comply with an agreed-upon security procedure that would have detected the error. The procedure may require a unique code for each payment order (to alert the receiving bank in the case of a duplicate payment), different codes for different levels of amounts, or identify regular beneficiaries. In order to benefit the sender, the security procedure, with which the receiving bank failed to comply, must have been agreed upon in advance. However, lack of compliance by the receiving bank with the agreed-upon security procedure, will not always save the sender; under UCC Section 4A-205(b), having been notified by the receiving bank of the acceptance of its payment order and having nevertheless negligently failed to timely discover and report an error, a sender may not shift the loss to the receiving bank which did not comply with the agreed-upon security procedure. Recovery of an erroneous payment resulting from an erroneous payment order is available to the receiving bank that bears the loss, but only to the extent allowed under the law of mistake and restitution.[193]

For its part, subject to one exception, PSD2 does not take a position on the responsibility for an erroneous payment order transmitted by the payer. The single exception is PSD2 Art. 88, which protects a payment service provider that acted in reliance on an incorrect unique identifier. Under PSD2 Art. 4(33), 'unique identifier' is defined to mean 'a combination of letters, numbers or symbols specified to the payment service user by the [PSP] and to be provided by the payment service user to identify unambiguously another payment service user and/or the payment account of that other payment service user for a payment transaction.' The simplest example is an account number. PSD2 Art. 88(1) deals with a payment order executed in accordance with a unique identifier. It authorizes a PSP to rely on the unique identifier so that 'the payment order shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier.'

It follows, and it is so provided in Art. 88(2), that the payment service provider that acted on the basis of the incorrect unique identifier provided by the user 'shall not be liable…for non-execution or defective execution of the payment transaction.' Moreover, under Art. 88(5), where the user furnishes the payment service provider with additional information to the unique identifier, 'the [PSP] shall be liable only for the execution of payment transaction in accordance with the unique identifier provided by the payment service user.' Under PSD2 Art. 88(3), having acted on the basis of the incorrect unique identifier, the PSP bears liability limited only to the making of 'reasonable efforts to recover the funds involved in the payment transaction,' an effort for which the PSP may charge the payment service user if it is agreed to in the framework contract.[194] PSD2 Art. 88(3) also requires the payee's PSP to cooperate in those efforts by communicating all relevant information for the collection of funds to the payer's PSP. In turn, where the recovery of the misdirected funds

[191] UCC Section 4A-208.

[192] UCC Section 4A-206.

[193] UCC Section 4A-205.

[194] See also PSD2 Art. 62(1) (including efforts to recover the funds as one of the 'corrective and preventive measures' for which the payment service provider may charge the payment service user).

is not possible, the payer's PSP shall provide to the payer all information available to it that is relevant to the payer in order for the payer to file a legal claim to recover the misdirected funds.[195]

One effect of PSD2 Art. 88 is that a PSP, which receives a payment order identifying a user by name and number, is free to act on the number alone. This goes, unnecessarily, further than UCC Art. 4A, which does not protect a PSP acting on the basis of the incorrect unique identifier with knowledge of the error or discrepancy.[196]

Finality of payment: completion of credit transfer and discharge of underlying debt

Under UCC Section 4A-104(a), a funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the originator's payment order. Acceptance by the beneficiary's bank further constitutes payment by the originator to the beneficiary, namely a discharge of the originator's obligation on the underlying transaction – that is, of the debt paid by means of the funds transfer.[197]

As indicated, acceptance by the beneficiary's bank is by making payment to the beneficiary or by advising the beneficiary either of receipt of the payment order or that the account of the beneficiary has been credited with respect to the order. In the usual case of a beneficiary's bank holding an account for the beneficiary, acceptance occurs by receiving payment from its sender.[198] Acceptance other than by payment to the beneficiary generates an obligation by the beneficiary's bank to pay the beneficiary.[199]

A beneficiary's bank that accepted a payment order, but failed to pay the beneficiary, may be held liable for the consequential (but foreseeable) loss.[200] Payment by the beneficiary's bank to the beneficiary can be made by crediting the beneficiary's account or in any other manner. Payment by crediting the beneficiary's account occurs upon notification to the beneficiary of the right to withdraw the credit, the lawful application of the credit to a debt of the beneficiary (whether to the beneficiary's bank or a garnishing creditor), or the availability of funds to the beneficiary.[201] Presumably, a beneficiary's bank crediting a final funds balance is to be taken as making funds available to the beneficiary even in the absence of further giving advice to the beneficiary.

In principle, payment by the beneficiary's bank to the beneficiary is final and cannot be made provisional or conditional on the receipt of funds from the sender.[202]

Art. 4A times the obligation of the beneficiary's bank to pay the beneficiary to coincide with the day of acceptance.[203] However, on this point, Art. 4A is pre-empted by federal law. The latter effectively provides that the beneficiary's bank must make funds available to the beneficiary no later than at the start of the next business day after the banking day of acceptance by means of receiving a sender's payment.[204]

Execution is dealt with in PSD2 Arts. 82-87. The term is, however, not defined in PSD2. From the heading to the chapter containing these provisions, referring to the execution of the payment transaction, as well from

---

[195] PSD2, supra n 44, Art. 88(3).

[196] Section 4A-207(b).

[197] UCC Section 4A-406.

[198] UCC Section 4A-209(b) and (c).

[199] UCC Section 4A-404 corresponding rule is provided for in MLICT Art. 10. UCC Section 4A-404 further requires the beneficiary's bank (at the risk of incurring liability for interest and possibly reasonable attorney's fees) to advise the beneficiary of a payment order instructing payment to the beneficiary's account before midnight of the next funds-transfer business day following the payment date (the latter being usually the day the order is received by the beneficiary's bank).

[200] UCC Section 4A-404(a). The beneficiary's bank avoids liability for such damages where it proves that it did not pay because of a reasonable doubt concerning the right of the beneficiary of the payment.

[201] UCC Section 4A-405.

[202] *Ibid*. No corresponding rule appears in the MLICT.

[203] UCC Section 4A-404(a).

[204] Reg. CC., Availability of Funds and Collection of Checks, 12 C.F.R. pt. 229 (1988), Section 229. 10(b)(1).

the context elsewhere in the Directive,[205] the term denotes the performance of the entire payment transaction, rather than carrying out the instruction contained in the payment order, as it does under UCC Art. 4A.[206] However, elsewhere in the Directive, reference is made to the execution of a payment order;[207] hence, the use of the term is inconsistent.

In the context of the completion of the payment transaction, PSD2 Art. 83 effectively addresses execution by reference either to the receipt of funds by the payee's payment service provider in the form of credit to its account or of crediting the payee's account by its payment service provider. In this context, it is not clear why receipt of funds by the payee's service provider is necessarily limited to the situation where funds are so received by means of credit posted to the account of the payee's payment service provider. Certainly, funds can be received by other ways – for example, by debit to the account of the payer's payment service provider.[208]

As indicated under PSD2 Art. 89(1), at the point in which the payer's payment service provider discharges its liability to the payer, 'the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction.' In turn, the liability of the payee's payment service provider to the payee is discharged by immediately placing the amount of the payment transaction at the payee's disposal and, where applicable, crediting the corresponding amount to the payee's payment account. The PSD does not address payment in cash to the payee. Nor does it address the point in the process in which the debt owed by the payer to the payee is discharged.

Liability for losses by a Receiving Bank

Under UCC Section 4A-305, the liability of a receiving bank for late or improper execution, as well as for non-execution in breach of contract, is limited to interest losses, expenses,[209] and in some circumstances, reasonable attorney fees. Except by express written contract, there is no liability for consequential loss, even foreseeable, including exchange losses, as well as a loss of a profitable contract due to the failure to meet a contractual payment deadline.[210] In the view of the drafters,[211] this rule is rationalized on the need "to effect payment at low cost and great speed."

PSD2 deals with the amount of liability, though not in a comprehensive manner. According to PSD2 Art. 89(3), '[PSP]s shall be liable to their respective payment service users for any charges for which [the PSPs] are responsible, and for any interest to which the payment service user is subject as a consequence of non-execution or defective, including late, execution of the payment transaction.' Under PSD2 Art. 91, any additional financial compensation 'may be determined in accordance with the law applicable to the contract concluded between the payment service user and the [PSP].' That is, in a departure from UCC Art. 4A, additional compensation—for consequential loss for example—is not rejected altogether, but its determination is to be made by reference to the law applicable to the relevant contract.[212]

Additionally, under limited circumstances, PSD2 Art. 92(1), provides recourse to a PSP liable to pay under PSD2 Art. 73 (for unauthorized payment) and PSD2 Art. 89 (for non-execution, defective or late execution of payment transactions). Losses are thus reallocated where liability for them is attributed to another PSP or an intermediary. In such a case, 'that [PSP] or intermediary shall compensate the … [PSP liable under Arts. 73 and 89] for any losses incurred or sums paid under Arts. 73 and 89,' including 'compensation where any

[205] See e.g. PSD2 Art. 4(13), under which: 'payment order' means an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction.

[206] UCC Section 4A-301(a).

[207] E.g. PSD2 Art. 79 dealing with the refusal of payment orders. See also PSD2 Art. 78(2).

[208] See '5. Sender's payment', id. discussing Section 4A-403 (enumerating several methods of interbank payment viz., through a funds transfer system, by crediting the receiving bank's account, by having the receiving bank debiting the sending bank account as well as netting and any other means).

[209] Expenses may not be recovered in the case of mere delay. See UCC Section 4A-305(a).

[210] This is an obvious departure from the common law rule of Evra v. Swiss Bank 673 F.2d 951 (7th Cir. 1982).

[211] Official Comment 2 to UCC Section 4A-305.

[212] UCC Section 4A-305.

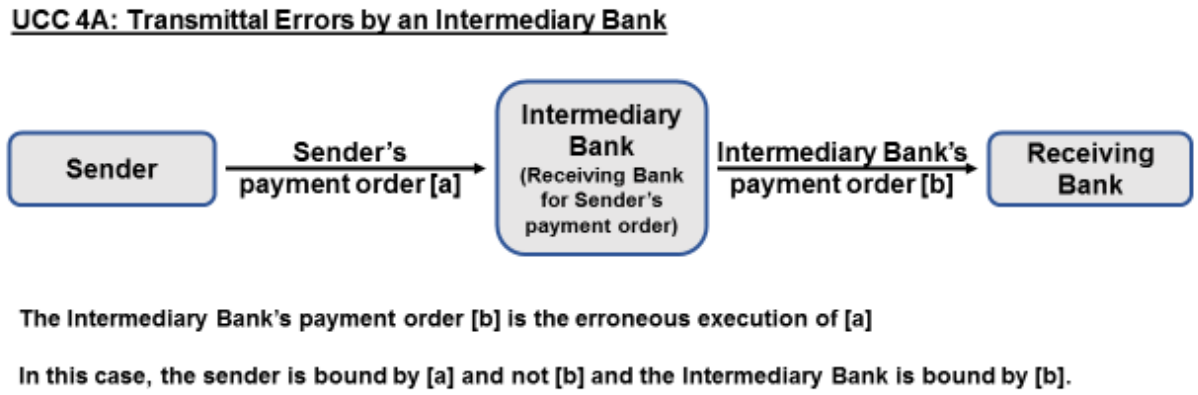
of the [PSP]s fail to use strong customer authentication.' Similar to PSD2 Art. 91, Art. 92(2) goes on to provide that '[f]urther financial compensation may be determined in accordance with agreements between [PSP]s and/or intermediaries and the law applicable to the agreement concluded between them.'

Numerous aspects of liability for losses are not dealt with by PSD2. This is the case in relation to whether an intermediary bank is liable directly to the payer and if so, whether such liability extends to consequential losses, as well as whether the payer's service provider is vicariously liable to the payer for consequential losses caused by an intermediary bank. This lack of treatment under the PSD is in contrast to Art. 4A, which excludes both intermediary bank's liability[213] and vicarious liability.[214]

Restitution upon erroneous completion of credit transfers

Under UCC Art. 4A, the sender is not responsible for the erroneous execution of its payment order by the issue of a non-conforming payment order by the receiving bank. A receiving bank executing the sender's order is required to issue a conforming payment order of its own.[215] Effectively, this means that the risk of erroneous execution is placed on the erring receiving bank.[216] For example, in case of overpayment resulting from the issue by the erring bank of a payment order in a larger amount than indicated in the one it received, the erring bank is required to pay the (larger) amount of its own payment order but is entitled to be paid only the (smaller) amount of the payment order is received.

Figure 12 Transmittal errors by an IB (UCC 4A)



In this scenario set out in Figure 12, the sender issued a payment order to its receiving bank ('Intermediary Bank') of which the content was [a]. The intermediary bank executed the 'sender's payment order' - [a]' by issuing its own payment order to the receiving bank – except that it was of a different content, i.e. [b]. In such a case, each issuer of a payment order is bound by the content of its own payment order. Accordingly, the sender is bound by [a] and the intermediary bank is bound by [b]. The difference between [a] and [b] may be in the sum to be paid, in the identity of the beneficiary, or the identity of the beneficiary's bank.

The following Figure 13 demonstrates the loss allocation where the difference between [a] and [b] is in the sum to be paid. In Figure 13, the originator instructed the originating bank to pay $100,000 to the beneficiary. The originating bank erroneously executed the originator's payment order by issuing to the intermediary bank a payment order in the sum of $1,000,000. The intermediary bank faithfully executed the originating bank's

[213] UCC Section 4A-212. This is so subject to interest liability and expenses under UCC Section 4A-305.

[214] UCC Section 4A-212. This is so subject to the money-back guaranty of Section 4A-402 discussed in # 3 supra.

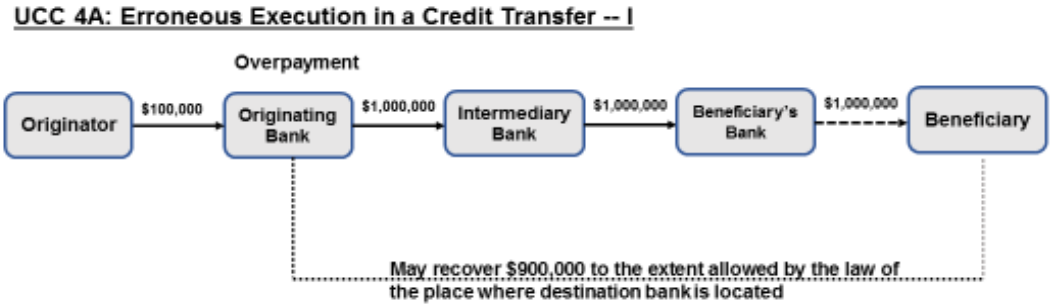
[215] UCC Section 4A-302.

[216] UCC Section 4A-303 dealing with erroneous execution leading to overpayment, underpayment or payment to a wrong beneficiary. The receiving bank is effectively exonerated where its non-conformance is in the selection of an intermediary bank other than that selected by the sender but the funds transfer is nevertheless completed without exception (so that in fact no loss occurred).

payment order and issued a payment order to the beneficiary's bank instructing payment of $1,000,000 to the beneficiary. The beneficiary's bank carried out this instruction faithfully so that beneficiary was paid $1,000,000.

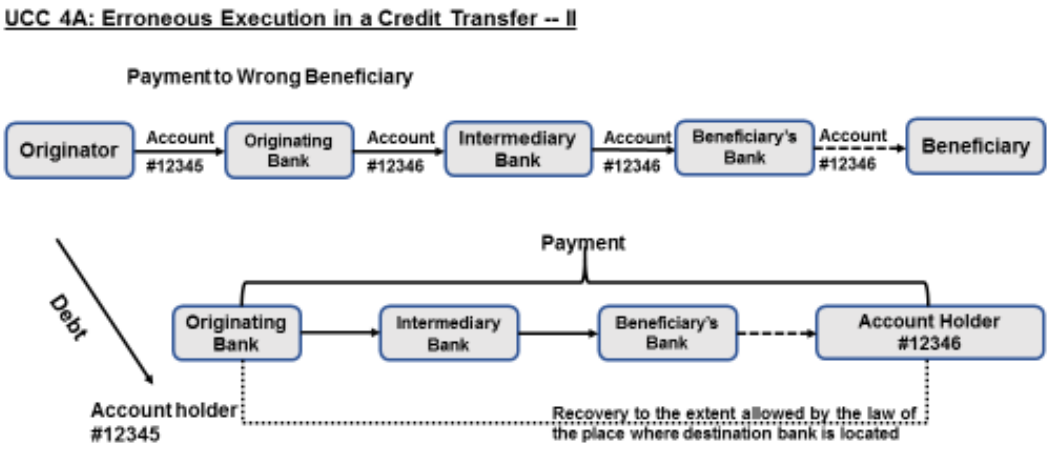
In this scenario, the originator owes the originating bank the sum of the originator's payment order which is $100,000. For their part, the originating bank owes the intermediary bank, and the intermediary bank owes the beneficiary's bank, $1,000,000, as each instructed. The loser is then the originating bank. While the beneficiary's bank may recover from intermediary bank, and the intermediary bank may recover from the originating bank, the $1,000,000 owed – the originating bank may recover only the $100,000 from the originator, but owes $1,000,000 to the intermediary bank. In such a case, the originating bank is allowed to recover the amount of its overpayment from the beneficiary, except that the general law of restitution may afford defences to beneficiary, as for example, upon change of position, or the discharge of another debt owed to beneficiary by originator.

Figure 13 Erroneous execution – overpayment



In another scenario the difference between [a] and [b] could be in the identity of the beneficiary. Thus, in Figure 14 below, the originator's payment order of content [a] - instructed the originating bank to carry out payment to originator's creditor, properly identified in the originator's payment order as account holder of account #12345 in the beneficiary's bank. The originating bank issued its own payment order to intermediary bank – in content [b] – instructing payment to the account holder of account #12346 at the beneficiary's bank. The intermediary bank duly executes as instructed, resulting in payment being made to account holder of account #12346. In this scenario, the originator, who remains liable to account holder of account #12345, is excused from liability to the originating bank while the latter is liable to the intermediary bank. The originating bank is left with an action against account holder of account #12346 – who, as in the previous scenario, may raise defences if and as available under the law of restitution.

Figure 14 Erroneous execution – payment to the wrong beneficiary



Indeed, a sender is obliged to pay the receiving bank the amount of its own payment order, albeit to the extent that the money-back guarantee rule does not apply. A sender of a payment order that is erroneously executed, who is notified by its receiving bank of the execution, and who was negligent in advising the receiving bank as to the error, does not forfeit any claim to a refund it may have against the receiving bank but is nevertheless not entitled to interest on the refunded amount.[217]

Recovery of an erroneous payment, resulting from erroneous execution, is available to the erring bank only directly from the actual beneficiary, even in the absence of privity between them. Such recovery can be made only to the extent allowed under the law of mistake and restitution.[218]

There are no corresponding provisions in PSD2.

Third-party intermediaries

Under UCC Section 4A-206(a),

> If a payment order[219] addressed to a receiving bank is transmitted to a funds-transfer system[220] or other third-party communication system for transmittal to the bank, the system is deemed to be an agent of the sender for the purpose of transmitting the payment order to the bank. If there is a discrepancy between the terms of the payment order transmitted to the system and the terms of the payment order transmitted by the system to the bank, the terms of the payment order of the sender are those transmitted by the system.

Stated otherwise, the third-party communication system is deemed to be an agent of the sender.

PSD2 is substantially more elaborate as it provides for two new types of payment services relating to payment initiation and account information.[221] Payment initiation service (PIS) is defined in Art. 4(15) as 'a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.' Account information service (AIS) is defined in Art. 4(16) as 'an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.' The providers of such services are called the payment initiation service providers (PISP) and the account information service provider (AISP), respectively.[222] The Directive covers both of the services, even to the extent that they may be viewed as technical service providers, which provide services supporting 'the provision of payment services, without them entering at any time into possession of the funds to be transferred.'[223] Such services are otherwise excluded under Art. 3(j). While PISPs and AISPs are not enumerated by the Directive as PSPs, they provide payment services, and as discussed below, are treated as payment institutions, which of course are PSPs.[224]

The functions of PISPs and AISPs in the provision of payment services and the rationale for their coverage by the Directive are set out in the PSD2 Preamble. Thus, paragraph 27 explains that a PIS 'play[s] a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's ASPSP in order to initiate internet payments on the basis of a credit transfer.'

---

[217] UCC Section 4A-304.

[218] UCC Section 4A-303.

[219] As well as a cancellations and amendment of a payment orders. See UCC Section 4-206(b).

[220] Defined in UCC Section 4A-105(3) to mean 'a wire transfer network, automated clearing house, or other communication system of a clearing house or other association of banks through which a payment order by a bank may be transmitted to the bank to which the order is addressed.'

[221] Points 7 and 8, respectively PSD2 Annex I.

[222] PSD2 Arts. 4(18) and (19), respectively.

[223] PSD2 Art. 3(j).

[224] PSD2 preamble, paragraph 26.

Under a new definition, Art. 4(17) defines an 'account servicing payment service provider' (ASPSP) to mean 'a payment service provider providing and maintaining a payment account for a payer.' The ASPSP is the PSP in which the payer's payment account is held. Effectively then, the PISP initiates a payment order at the request of the payment service user, as the payer, out of a payment account the payer has with the ASPSP. Paragraph 29 of the Preamble further explains,

> [PIS]s enable the [PISP] to provide comfort to a payee that the payment has been initiated in order to provide an incentive to the payee to release the goods or to deliver the service without undue delay. Such services offer a low-cost solution for both merchants and consumers and provide consumers with a possibility to shop online even if they do not possess payment cards.

On the other hand, paragraph of the Preamble also explains that the lack of coverage to PIS would have 'raise[d] a series of legal issues, such as consumer protection, security and liability as well as competition and data protection issues.'

For its part, paragraph 32 of the Preamble elaborates on the modes of access by a PISP to the payer's payment account held at the ASPSP as follows:

> [PIS]s are based on direct or indirect access for the [PISP] to the payer's account. An [ASPSP] which provides a mechanism for indirect access should also allow direct access for the [PISP]s.

In a direct access mode, known as screen scraping, the PISP uses the customer's account login and accesses the customer's account, exactly as the customer would do, via the ASPSP's webpage. Alternatively, in the indirect access mode, the ASPSP provides the PISP account access through a dedicated application programming interface (API).[225] Regulatory standards favour the latter, which, unlike the former, is capable of limiting the data accessed by the PISP to only what is required for provision of the service.[226]

The need to regulate both PISPs and AISPs, particularly by reference to their position towards the ASPSP, is explained by the PSD2 Preamble in paragraph 93 as follows:

> It is necessary to set up a clear legal framework which sets out the conditions under which [PISP]s and [AISP]s can provide their services with the consent of the account holder without being required by the [ASPSP] to use a particular business model, whether based on direct or indirect access, for the provision of those types of services. The [PISP]s and the [AISP]s on the one hand and the [ASPSP] on the other, should observe the necessary data protection and security requirements established by, or referred to in, this Directive or included in the regulatory technical standards. Those regulatory technical standards should be compatible with the different technological solutions available. In order to ensure secure communication between the relevant actors in the context of those services, EBA should also specify the requirements of common and open standards of communication to be implemented by all [ASPSP]s that allow for the provision of online payment services. This means that those open standards should ensure the interoperability of different technological communication solutions. Those common and open standards should also ensure that the [ASPSP] is aware that he is being contacted by a [PISP] or an [AISP] and not by the client itself. The standards should also ensure that [PISP]s and [AISP]s communicate with the [ASPSP] and with the customers involved in a secure manner. In developing those requirements, EBA should pay particular attention to the fact that the standards to be applied are to allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services.

[225] An API is a software intermediary that allows two applications to talk to each other. Shana Pearlman, "What are APIs and how do APIs work" (September 07, 2016), online (blog): <https://blogs.mulesoft.com/biz/tech-ramblings-biz/what-are-apis-how-do-apis-work/>, accessed 5 March 2020.

[226] See in general: Markus Demary & Christian Rusche, "Strengthened Competition in Payment Services 4" (IW-Kurzbericht, No. 4/2018, 2018), online:<https://www.econstor.eu/bitstream/10419/173454/1/101095413X.pdf>, accessed 5 March 2020.

To obtain authorization, PISPs and AISPs are required to 'hold a professional indemnity insurance, covering the territories in which they offer services, or some other comparable guarantee against liability.'[227]

In relation to capital requirements, PISPs are categorized as payment institutions. More directly, Art. 33(2) mandates that AISPs shall be treated as payment institutions. However, Article 33(2) further states that Titles III and IV shall not apply to AISPs," other than specified provisions addressing information requirements (Art. 45 and 52); burden of proof as to compliance with information requirements (Art. 41); rules on access to and use of payment account information in the case of account information services (Art. 67); obligations of the payment service user in relation to payment instruments and personalized security credentials (Art. 69); and operational and security risks and authentication (Arts. 95-98). Art. 33(1) further relaxes the application of rules governing applications for authorization (Art. 5) and registration (Art. 15).

Paragraph 33 of the PSD2 Preamble states that '[a]ny payment service provider, including the [ASPSP] of the payment service user, should be able to offer [PIS]s.' As for the access of a PISP to the payer's funds, and position vis-à-vis the ASPS, paragraph 30, explains,

> The personalized security credentials used for secure customer authentication by the payment service user or by the [PISP] are usually those issued by the [ASPSP]s. [PISP]s do not necessarily enter into a contractual relationship with the [ASPSP]s and, regardless of the business model used by the [PISP]s, the [ASPSP]s should make it possible for [PISP]s to rely on the authentication procedures provided by the [ASPSP]s to initiate a specific payment on behalf of the payer.

In rationalizing the application of the Directive to AISs, paragraph 28 of the Preamble explains that they 'provide the payment service user with aggregated online information on one or more payment accounts held with one or more other [PSP]s and accessed via online interfaces of the [ASPSP].' They thus enable the payment service user 'to have an overall view of its financial situation immediately at any given moment.' In this context, the Directive coverage is thus required 'to provide consumers with adequate protection for their payment and account data as well as legal certainty about the status of [AISP]s'.

Law applicable: variations and cross-border- international setting

Under UCC Art. 4A, to some extent, a rule adopted by a funds-transfer system (funds transfer system rule), and to a lesser extent, even a bilateral agreement, may supersede the provisions of Art. 4A.[228] At the same time, PSD Art. 51 gives more leeway to contracting parties to exclude the provisions of the Directive. Thus, in non-consumer payment transactions, parties may contract out of provisions dealing with allocation of charges (Art. 52(1)); authorization by consent by means of an agreement (Art. 54(2)); time for notifying an unauthorized or incorrectly executed payment transaction (Art. 58); onus of proof in connection with an alleged unauthorized payment transaction (Art. 59); allocation for losses for unauthorized payments (Art. 61); refund for debit transfers (Arts. 62 and 63); irrevocability of a payment order (Art. 66); and loss allocation in connection with non-execution or defective execution (Art. 75).

Under Art. 4A, unless displaced by a bilateral agreement or a funds-transfer system rule, the law applicable to each payment order is that of the jurisdiction in which the receiving bank is located. Similarly, the law of the jurisdiction in which the beneficiary's bank[229] is located governs the relationship between the beneficiary's bank and the beneficiary, as well as the discharge of the originator's debt to the beneficiary. A funds transfer system rule, displacing any of the above, binds all participants to a funds transfer having notice that the funds-transfer system might be used in the funds transfer and of the choice of law made by the system. In the United States, both CHIPS and Fedwire effectively selected Art. 4A as the governing law. However, as indicated, unless displaced by either a funds transfer system rule or bilateral agreement, applicable law is

[227] PSD2 Arts. 5(2)-(3).

[228] UCC Section 4A-501. Federal Reserve regulations and operating circulars supersede inconsistent provisions of Art. 4A under UCC Section 4A-107. For a detailed discussion on the power of parties to vary the provisions of UCC Art. 4A, see Benjamin Geva, The Law of Electronic Funds Transfers (Matthew Bender Elite Products, looseleaf: updated to 2019) at §2.06.

[229] For both situations, note that under UCC Section 4A-105(a)(2), "A branch or separate office of a bank is a separate bank for purposes of this Article".

determined under Art. 4A by reference to each individual bilateral relationship (that is, sender-receiving bank, beneficiary's bank-beneficiary, and originator-beneficiary) and not the entire funds transfer.[230]

PSD2 Art. 2(1) provides for the territorial scope of PSD2 as follows:

> The Directive applies to payment services provided within the EU.[231]

However, PDS2 Art 2 goes on to provide for special rules to govern the scope of Titles III and IV. These titles respectively deal with the transparency of conditions and information requirements for payment services, and rights and obligations in relation to the provision and use of payment services. By way of summary, depending on the currency in which payment is to be made,

(a) For payment transactions in the currency of a Member State, Title III and IV apply 'where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union';[232]

(b) For 'payment transactions in a currency that is not the currency of a Member State', Titles III and IV apply 'where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union,' albeit only 'in respect to those parts of the payments transaction which are carried out in the Union.'[233] However, a few exceptions exist. Thus, there is no requirement in relation to the maximum execution time, value date, and deductions from the amount transferred (under PSD2 Articles 45(1), 52(2)(e), 56(a), and 81–86);[234] and

(c) For 'payment transactions in all currencies', Titles III and IV apply 'where only one of the payment service providers is located within the Union', albeit only 'in respect to those parts of the payments transaction which are carried out in the Union.'[235] Exceptions similar to those of its predecessor exist, plus additional ones as, for example, in respect to refunds for payment transactions initiated by or through a payee and liability.

Concluding Observations

All over the world, the credit transfer, in its electronic form, has come to supersede the paper-based cheque, so as to dominate to a large extent the non-cash payment landscape. Addressing the various legal issues arising in connection with this method of payment is a challenge even in the developed world. For developing countries with weaker legal and banking traditions, the challenge is higher. Hence, adaptations of legislation passed in leading developed countries may be extremely helpful in any legal and regulatory reform.

[230] For these choices of law rules, see UCC Section 4A-507. For the broader picture, see e.g. Luca G. Radicati di Brozolo, "International Payments and Conflicts of Laws" (2000) 48:2 Am J Comp Law 307.

[231] "Institutions referred to in points (4) to (23) of Art. 2(5) of Directive 2013/36/EU" may be exempt by their Member state from the application of all or part of the provisions of PSD2. PSD2 Art. 2(5).

[232] PSD2 Art. 2(2).

[233] PSD2 Art. 2(3).

[234] See generally PSD2 Arts. 45(1), 52(2)(e), 56(a), 85-86.

[235] PSD2 Art. 2(4)