# A Critical Examination of Aspects of Liability for Fraudulent Electronic Funds Transfer in English, US and EU Law with Particular Reference to the UNCITRAL Model Law

**Thesis submitted for the degree of**
**Doctor of Philosophy**
**at the University of Leicester**
**by**

**Muna Nimer**
**Faculty of Law**
**University of Leicester**
**June 2007**





ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

To my beloved mother.

## ABSTRACT

This thesis argues that the scope of the originator and the originator's bank's rights, duties and liabilities for international fraudulent wholesale EFT under English law, is unpredictable and uncertain.

The argument relies on analysing the law applying to fraudulent international wholesale EFT in England. This includes the general principles of contract law, agency law and the rules which apply to forged cheques, and the UK Cross-Border Credit Transfer Regulations 1999 which implemented the EU Directive on Cross-Border Credit Transfers 1997. The English law is then compared with Article 4A of the U.S. Uniform Commercial Code 1989 and the UNCITRAL Model Law in International Credit Transfer 1992.

This thesis demonstrates that because of the distinctive nature of EFT authentication, applying English common law to international fraudulent wholesale EFT gives rise to significant legal problems. Namely, the problem of identity authentication, the unfair allocation of loss between the originator and the originator's bank for fraudulent payment orders, problems about the standard of security procedures to be implemented to authenticate the originator's instructions, the use of unfair contract terms by the originator's banks in their contract to exclude or limit their liability for fraudulent EFT, and the unpredictability and uncertainty of scope of the originator's bank's liability for direct and consequential damages occurring as a result of fraudulent EFT. Moreover, this thesis illustrates that the UK Cross-Border Credit Transfer Regulations and the EU Directive on Cross-Border Credit Transfer are not comprehensive and sophisticated, as they do not deal with the above mentioned problems in the context of fraudulent EFT. Moreover, this legislation is limited in its application as it applies only to EFT up to 50,000 Euros and to EFT executed between EU Member States. This thesis concludes that there is a need for a new regulatory frame work deal with the above-mentioned problems in the context of international fraudulent wholesale EFT.

# TABLE OF CONTENTS

## CHAPTER TWO
## ANALYSIS OF THE LAW RELATING TO UNAUTHORISED INTERNATIONAL WHOLESALE ELECTRONIC FUNDS TRANSFER IN ENGLISH LAW AND EU LAW

## CHAPTER THREE
## EXAMINTION OF THE UNCITRAL MODEL LAW AND ARTICLE 4A IN THE CONTEXT OF UNAUTHORISED EFT

## CHAPTER FOUR
## PARTIES' LIABILITIES FOR FRAUDULENT INTERNATIONAL WHOLESALE ELECTRONIC FUNDS TRANSFER IN ENGLISH AND EU LAW

## CHAPTER FIVE
## PARTIES' LIABILITY FOR INTERNATIONAL FRAUDULENT WHOLESALE EFT UNDER THE UNCITRAL MODEL LAW AND ARTICLE 4A

## CHAPTER SIX
## CONCLUSION



## Bibliography

# ACKNOWLEDGEMENTS

First of all, I would like to thank my mother for all her unceasing help and support, I am very grateful to her. My brothers and sister have also been very supportive and helpful. I am very grateful to both my supervisors Mr. Ian Snaith and Dr. Lorna Gillies for their patient and thorough reading of my work. I would not have been able to finish this work without their constant encouragements and comments on draft after draft of my work. My sincere thanks go to Dr. Kamal Naser, who encouraged me to embark upon a PhD. He helped me in establishing the main ideas of this study, which I am most grateful. My gratitude for Dr. Rateb Swies, who has helped enormously throughout my research with his advice and continuous support. Special thanks go to Professor Panu Minkkinen for his precious advice and invaluable support. Finally many thanks to all my friends and colleagues from Jordan or Britain or from more distant places, who have always been supportive and encouraging with their dialogue.

# INTRODUCTION

In October 2004, EU Internal Market Commissioner Frits Bolkestein stated:

> "[W]ithout secure payment systems, you cannot have a modern economy or a functioning Internal Market. In the EU, payment fraud is exceeding €1 billion annually. Fraudsters come up with new scams and the payment industry needs to stay one step ahead. That means vigilance and reinforced cooperation within and beyond the EU." [1]

Since 1970, information technology has had a significant influence on international electronic banking activities, [2] which facilitate the movement of money across the world between banks and their customers. [3] There is a consensus in the literature that information technology has affected various areas of banking activities, [4] for instance the type of the financial services the bank offers its customer to transfer funds electronically within the same borders, or internationally. The emergence of the Internet has increased both the number and size of international financial transactions, and has enhanced the globalisation of banking business. [5] International wholesale electronic funds transfer (hereafter EFT) is a type of international financial transaction that is executed over the Internet between banks and their customers. [6]

---

[1] "Payment Fraud: Commission sets out Battle Plans," Out-Law. Com/ News, 28/10/2004. http://www.out-law.com/page-5017, http://www.out-law.com (obtained on 13/10/2005).

[2] Donal O' Mahony, Micheal Peirce, and Hitesh Tewari, *Electronic Payment systems for E-Commerce* 2nded, Boston, Mass, 2001 at p.1.

[3] Norbert Horn, *Legal Issues in Electronic Banking*, Kluwer Law International, The Hague; London 2002 at p.3-5, Paul S. Tufaro, and William H. Boger, " Electronic Banking in the United States: Evolution not Revolution," C.T.L.R. 1997, 3(2), 70-75, Ramin Cooper Maysami, and Kim Mills, "Regulation and Supervision of Online Banking Services in the United States: an Integrated Approach," J.I.B.L.R. 2004, 19 (11), 447-454, at p.447, Barry B Sookman, Electronic Commerce, Internet and the Law- Survey of the Legal Issues: Part 1," C.T.L.R. 1999, 5 (2), 52-58 and UNCTAD,"E-Commerce and Development Report 2002," United Nations, New York, 2002, pp.133-136.

[4] Horn, ibid, Maysami and Mills ibid, Sookman, ibid and UNCTAD report 2002, ibid.

[5] Horn, ibid at p. 5.

[6] Internet Banking: Comptroller's Handbook, Comptroller of the currency Administrator of national banks, (hereafter Internet Banking Comptroller's Handbook) October 1999 at p.1. http://www.occ.treas.gov/handbook/intbank.pdf http://www.occ.treas.gov (obtained 25/4/2004).

The benefits of using electronic means such as the Internet or dedicated networks to execute funds transfers between banks and customers are significant. [7] First, the money can be transferred faster and the settlement between accounts can be executed almost instantly. [8] Second, there is a cost reduction of funds transfer to the bank and the customer, in comparison with paper-based means [9] such as cheques. Lastly, customers can access their accounts and generate payment orders from their offices. [10] Therefore, international wholesale EFT is a very popular means of transferring money between financial institutions, banks and business customers in financial markets across the world. [11] Sappideen affirms that international wholesale EFT has significantly influenced the economy and financial services at international level. [12] Consequently, international wholesale EFT is an extremely important method to facilitate and promote international business transactions. [13] In 2006 the estimated daily value of EFT (large values) in UK through CHAPS [14] Sterling was £235,863 million and £28.885 million between members of CHAPS Euro. Moreover, in 2006

---

[7] Hal S. Scott, " Corporate Wire Transfers and the Uniform New Payments Code," 83. Colum. L. Rev. 1664 at p.1664, Hyung J. Ahn, " Note Article 4A of the Uniform Commercial Code: Dangers of Departing from a Rule of Exclusivity," 85 Va. L. Rev. 183, Feb 1999 at p. 184 and Mary Donnelly, "Electronic Funds Transfers: Obligations and Liabilities of Participating Institutions," C. L. Pract. 2003, 10 (2), 35-39. at p. 35

[8] Donnelly, ibid and Ahn, ibid at p.183.

[9] Ahn, ibid and Internet Banking Comptroller's Handbook, note 6 supra at p.3.

[10] Mark Hapgood, QC, *Paget's Law of Banking* 12th ed, Butterworths, London 2002 at p. 329 and Ahn, ibid.

[11] Razeen Sappideen, "Cross-Border Electronic Funds Transfers Through Large Value Transfers Systems and the Persistence of Risk," 2003, J.B.L., pp.584-602 at p.584 and Raj Bhala, " International Payments and Five Foundations of Wire Transfer Law," Essays in International Financial & Economic Law No, 2, International Finance and Tax Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, University of London, in cooperation with the London Centre for International Banking Studies and the London Institute of International Banking, Finance and Development Law, London, 1996 at pp.6-7

[12] Sappideen ibid.

[13] Sappideen ibid and Bhala, note 11 supra at pp. 6-7.

[14] The large value payment systems currently existing in UK, US and EU are CHAPS in UK, FEDWIRE and CHIPS in the US and TARGET in EU. FEDWIRE and TARGET are payment systems owned and managed by the central banks in these countries. CHIPS and CHAPS on the other hand are payment systems owned and managed by payments association. Under these systems settlement occurs on either a gross or a net basis. FEDWIRE, CHAPS and TARGET are real time gross settlement systems (RTGS), in comparison to CHIPS, which is a netting-based system. It is important to bear in mind that each system has its own rules, which regulate the members' duties, liabilities and choice of law. However, the relationship between these systems' rules and the originator and the originator's bank falls outside the ambit of this thesis.

the estimated daily value of EFT transmitted to TARGET from UK was £83.980 million, and from TARGET to UK £83.997 million.[15] Meanwhile in 2006, the daily value of CHIPS funds transfer in US was estimated at $1,571,981,296. [16]

The aim of this thesis is to examine the scope of the liability of the originator's bank and the originator for fraudulent international wholesale EFT under English law, US law, EU Law and the UNCITRAL Model Law in International Credit Transfer 1992 (hereafter the UNCITRAL Model Law). [17] This will be achieved by examining and assessing the UNCITRAL Model Law and Article 4A of the Uniform Commercial Code 1989 [18] in the US (hereafter Article 4A) compared with the general principles of contract law, agency law and the rules which apply to forged cheques in England. As Article 4A has influenced the UNCITRAL Model Law, this thesis examines the differences between them in the context of fraudulent international wholesale EFT where applicable. Furthermore, the thesis demonstrates that the EU Directive 97/5/EC of the European Parliament and of the Council on Cross-Border Credit Transfers [19] (hereafter EU Directive) is inadequate and inappropriate to deal with fraudulent international wholesale EFT. Accordingly, this thesis examines the purposes and the scope of the EU Directive. Moreover, the thesis examines the Cross-Border Credit Transfer Regulations 1999 [20] in UK (hereafter UK Regulations), which implemented the EU Directive in the UK. In short, the aim of this thesis is to conduct and produce

---

[15] "Annual Summary of Clearing Statistics 2006," Facts and Figures, Annual Clearing Statistics. http://www.apacs.org.uk/resources_publications/documents/annsumm06.pdf (obtained on 08/02/2007)
[16] CHIPS Annual Statistics from1970 to 2007. http://www.chips.org/about/pages/000652.php (obtained 08/02/07).
[17] UNCITRAL Model Law in International Credit Transfer 1992. http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf
[18] Article 4A of the Uniform Commercial Law 1989. http://www.law.cornell.edu/ucc/4A/ (obtained on 08/02/2007).
[19] Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, OJ L 043, 14/02/1997 P. 0025 – 0030.
[20] Cross-Border Credit Transfer Regulations 1999, SI1999 No 1876.

an assessment of the above-mentioned laws governing fraudulent international wholesale EFT, and to provide suggestions for the way forward in England.

In regards to the assessment, this thesis will demonstrate that in England, the rules of contract law, agency law and the rules that apply to forged cheques are inadequate and incapable of solving the problems of fraudulent EFT. Firstly, there is the problem of identity authentication and the difficulty of determining whether the payment order is authorised or not. In EFT it is difficult to identify the person who sends the payment order, because of the lack of the face-to-face connection, it is difficult to determine whether the person who sends the payment order is authorised to do so or not. This thesis will demonstrate that applying agency law and the rules apply to forged cheques leads to the conclusion that the bank will be liable for an authenticated, but unauthorised payment order. Secondly, the scope of the originator's bank's liability for direct damages, consequential damages and interest in the context of fraudulent EFT is uncertain and unpredictable. Further, this thesis will demonstrate that the EU Directive and the UK Regulations' rules are limited in their application in terms of the payment order value, and do not treat all the problems that may arise in EFT, such as fraud. The existing rules mentioned above as applying to EFT are neither adequate nor capable of solving the problems that arise in cases of fraudulent wholesale EFT. This thesis argues that the EU Cross-Border Credit Transfer Directive and the UK Regulations should be amended in order to regulate and govern the problems arising from wholesale fraudulent EFT and without limitation to the payment order value. Amendments need to be made by incorporating rules to determine whether the payment order is authorised or not, in order to avoid the problem of identity authentication and its consequences on the parties' liabilities under agency law and the rules applicable to forged cheques. Equally important, the amendment should

incorporate rules which determine the scope of the parties' rights, duties and liabilities in the context of a fraudulent EFT, such as the banks' liability for direct losses, consequential losses and interest. Since the UK Regulations implemented the EU Directive and the EU Directive has been influenced by the UNCITRAL Model Law, the rules of the UNCITRAL Model Law which apply to fraudulent EFTs should be compared with the EU directive and UK Regulations.

The approach followed in this thesis is that the examination of the originator's bank and the originator's liability should start by explaining the meaning of fraud in the context of an international wholesale EFT. The purpose of chapter one is to set out the basic context and definitions necessary to clear the way for a fuller analysis in subsequent chapters. Thus, chapter one in section 1.2.1 starts by defining EFT for the purposes of this thesis and demonstrating the difference between paper-based funds transfer and EFT. Section 1.2.2 demonstrates the legal concept of international wholesale EFT as it is significant in distinguishing between the law that applies to wholesale and retail EFT s. Then, section 1.2.3 focuses on particular problems related to fraudulent EFT and why this thesis confines itself to fraudulent EFT's. Furthermore, section 1.2.4 considers the concept of fraudulent EFT under English common law. This section seeks to illustrate when fraud occurs, and the potential types of fraud in the context of EFT. Finally, section 1.2.5 explores the significance of authority under agency common law in the context of EFT in order to determine whether the payment order is an authorised or an unauthorised payment order. This section demonstrates how the application of the common law rules of agency to EFT raises the problem of identity authentication as a result of the distinctive nature of authentication, in the case of an electronic payment order.

Chapter two analyses the law that applies to unauthorised international wholesale EFT in English law and EU law, namely the law of agency, the law of contract, the EU Directive and the UK Regulations. This demonstrates that these laws are neither adequate, nor efficient in dealing with the problems related to fraudulent EFT, in particular the problem of identity authentication and whether an authenticated payment order is an authorised payment or not. Section 2.2 considers the legal nature of funds transfer in English common law to determine the law that applies to such transactions. Section 2.2 concludes that EFT is an authority conferred by the originator to the originator's bank to debit his account and credit the beneficiary's account. Accordingly, the law of agency and the law of contract govern the parties' rights, duties and liabilities in the context of fraudulent EFT. Following this, section 2.3 critically examines the application of the law of contract and the law of agency to unauthorised EFT to demonstrate that the application of such rules leads to unpredictability and uncertainty of the parties' rights, duties and liabilities for fraudulent EFT. This is because the law of contract and the law of agency law cannot deal with the problems of identity authentication and the unfair terms imposed on the originator by the originator's bank. Furthermore, section 2.4 analyses the EU Directive on cross-border credit transfer and its application to EFT. The analysis demonstrates that the scope of the EU Directive application is narrow, as it applies only to funds transfer up to 50,000 euros and does not deal with fraudulent EFT. Section 2.4 considers the UK regulations on cross-border credit transfer. This section examines the scope of the UK Regulations, which will show that the scope of the UK Regulation is limited as it applies to funds transfer 50,000 euros and to funds transfer within the EU. Moreover, section 2.4 illustrates that the UK Regulations do not

regulate the parties' rights, duties and liabilities for fraudulent EFT and the same applies to the EU Directive. Thereby, sections 2.4 and 2.5 show that the EU Directive and the UK Regulations need to be amended to regulate the parties' rights, duties and liabilities for fraudulent EFT. Section 2.6 focuses on the Jack Committee report. Although it has been a long time since the report was published, it is still significant, because it highlighted the important problems arising in the context of EFT and the need for rules to regulate these problems, namely, that the problems of identity authentication, the security procedures used to authenticate the electronic payment orders and the parties' liabilities for such transactions should not be left entirely to contractual arrangements. Finally, Chapter two in section 2.7 examines the legal validity of the security procedures in English law and the forms of security procedures used to authenticate EFT. The examination considers English common law and the EU Directive on E-signature and its implementation in England. The purpose of section 2.7 is to demonstrate that the above-mentioned legislation does not yet solve the problem of identity authentication and the originator and originator's bank liability for authenticated but unauthorised payment orders. Chapter two argues that the problems of identity authentication, the parties' liabilities for authenticated but unauthorised payment order and the standard of security procedure used to authenticate electronic payment order need to be regulated by particular rules. Such rules should be added to the UK regulations, and these rules must take into consideration the distinctive nature of authentication of electronic payment orders which differ from the method used to authenticate paper-based payment orders.

Chapter three examines the UNCITRAL Model Law and Article 4A treatment of unauthorised EFT to consider whether the originator and the originator's bank's liabilities for authenticated but unauthorised payment order is more predictable and certain than under English law. Moreover, chapter three considers how the UNCITRAL Model Law and Article 4A have solved the problems of identity authentication in the context of fraudulent EFT. Thus, section 3.2 of this chapter starts with background and historical basis of the UNCITRAL Model Law. Then section 3.2 examines the rules of the UNCITRAL Model Law apply to unauthorised EFT. The examination demonstrates that the originator and the originator's bank's liabilities for authenticated but unauthorised payment orders are predictable and certain. Finally, section 3.2 illustrates that according to the rules of The UNCITRAL Model Law the standard of security procedures that should be implemented to authenticate the originator's payment orders. Then, section 3.3 deals with the rules of Article 4A as they apply to unauthorised EFT. Section 3.3 considers the rationale behind adopting Article 4A, and demonstrates that before Article 4A it was found that applying the general principles of contract law, agency law and case law was not adequate in dealing with unauthorised EFT. Furthermore, section 3.3 assesses the rules of article 4A that govern and regulate unauthorised EFT. The assessment shows that Article 4A has devoted particular rules to solving the problem of identity authentication; consequently the originator and the originator's bank's liabilities for authenticated but unauthorised payment order are predictable and certain. Finally, section 3.3 examines the rules of Article 4A which determine the standard of security procedures should be implemented by the originator's bank to authenticate the originator's payment orders. This section considers the originator's bank duty to implement "commercially reasonable" security procedures and its effect on the originator and the originator's

bank's liabilities for authenticated but unauthorised payment orders. Chapter three concludes by arguing that the UNCITRAL Model Law and Article 4A's solution for the problem of identity authentication leads to predictability and certainty in the originator and the originator's bank's liability for authenticated but unauthorised payment orders.

Chapter four attempts to examine the originator and the originator's bank's liabilities for fraudulent EFT in England and the EU to demonstrate that applying the rules of agency law and contract law to the originator and the originator's bank's liabilities leads to uncertainty and unpredictability. Furthermore, chapter four examines the rules of the EU Directive and UK Regulations in the context of fraudulent EFT. The examination will show that the UK Regulations and the EU Directive are limited in their application and are not comprehensive as they do not set out particular rules for authorized and unauthorized payment order or the parties' liability for such fraudulent transactions. Accordingly, this section argues that the originator and the originator's bank's liabilities for fraudulent EFT need to be regulated by particular rules. Furthermore, chapter four argues that EU Directive and UK Regulations need to be amended to regulate the parties' liabilities for fraudulent EFT and regardless of the pecuniary amount of the funds transfer. Thus, section 4.2 deals with the basis of the originator's actions against the originator's bank for fraudulent EFT in England. Section 4.3 examines the originator's liability for fraudulent EFT when his negligence facilitates fraudulent EFT. Section 4.3 considers the scope of the originator's bank liability for fraudulent EFT as a result of its negligence. Section 4.4 examines the scope of the originator's bank's liability for direct damages and consequential damages occur as a result of fraudulent EFT. Section 4.5 deals with the originator's

bank's liability for failed payment orders under the EU Directive and UK Regulations on Cross-Border Credit Transfers. Finally, section 4.5 discusses the view of the Jack Committee Report on the parties' liability for fraudulent EFT.

Chapter five evaluates those rules of the UNCITRAL Model Law and Article 4A that regulate and govern the originator and the originator's bank's liabilities for fraudulent EFT. This chapter demonstrates that the originator and the originator's bank's liabilities for fraudulent EFT are more predictable and certain than under English law. Furthermore, chapter five argues that the EU Directive and UK Regulations need to be amended by adding rules regulate the originator and the originator's bank's liabilities for fraudulent EFT. Sections 5.2 and 5.3 examine the rules of the UNCITRAL Model Law and Article 4A that apply to originator and the originator's bank's liabilities for fraudulent EFT respectively. 5.2.1 and 5.3.1 sections deal with the significance of the parties' agreement on the security procedures implemented to authenticated the originator's payment order. These sections will demonstrate the effects of such an agreement on the originator and the originator's bank's liabilities for fraudulent EFT. Furthermore, sections 5.2.2 and 5.3.2 examine the originator and the originator's bank's liabilities for fraudulent EFT when the fraudulent payment order was issued by different persons. For example, when the payment order is issued by one of the originator's employees, or by one of the originator's bank's employees or by a third party. These sections demonstrate that the parties' liability for fraudulent EFT is determined according to the person who issues the payment order. Moreover, sections 5.2.3 and 5.3.3 deal with the scope of the originator's bank's liabilities for direct damages and consequential damages occur as a result of fraudulent EFT, to demonstrate that the originator's liabilities are more predictable and certain than under

English Law. Following this, sections 5.2.4 and 5.3.4 examine the originator's basis of action against the originator's bank and freedom of contract to demonstrate that under the UNCITRAL Model Law and Article 4A the freedom of contract is subject to mandatory rules to protect the originator from unfair contract terms. Finally, section 5.3.5 deals with the originator's duty to notify the originator's bank of fraudulent EFT and the "Statute of Repose". To demonstrate that such a duty makes the originator's bank's liability for fraudulent EFT predictable and certain.

The way forward and a conclusion to these chapters complete this research. The way forward and the conclusion contain some of the present author's views and suggestions as to the research subject but not all of them, as more detail regarding such views and suggestions will be discussed with the specific issues through out the thesis. The main purpose of this chapter is to recollect and reemphasis the main problems and the suggestions for possible solutions for such problems. The main problem this conclusion chapter attempts to answer is whether the law in England governing EFT is currently adequate and appropriate in dealing with fraudulent EFT, especially in the absence of statute law or regulations in England governing EFT. Thus, the question of whether a statutory law or regulations regulate EFT is needed in England will be discussed.

# CHAPTER ONE

# FRAUD AND INTERNATIONAL WHOLESALE FUNDS TRANSFER LAW

## 1.1. INTRODUCTION

EFT activities are growing considerably day by day in the UK. Statistics show that in 2005, the total value of funds transfers cleared through CHAPS was £97.100.206 million. By 2006, the figure had grown to £109.100.206 million. [1] Money can be transferred electronically in huge or trivial sums by using different methods, such as, ATM, credit card, debit card, e-cheque and credit transfer. [2] This thesis focuses on one type of EFT, that is of international wholesale EFT. Furthermore, this thesis is devoted to examining the originator and the originator bank's rights, duties and liabilities for fraudulent international wholesale EFT. Accordingly, section 1.2 of this chapter sets out the central concepts and definitions of international wholesale EFT. Section 1.2.1 demonstrates the difference between paper-based funds transfer and EFT. Then, section 1.2.2 discusses the legal concept of international wholesale EFT, as it is important to determine which rules apply to such transactions. Section 1.2.3 focuses on particular problems related to fraudulent EFT and why the thesis focuses of fraudulent EFT's. Section 1.2.4 explores the concept of fraud in the context of the EFT in English law. Moreover, section 1.2.4 examines the potential types of fraud in the context of EFT. Then, section 1.2.5 considers the significance of authority in the

[1] APACS the UK Payment s Association, "Annual Summary of Clearing Statistics 2006," Facts and Figures, Annual Clearing Statistics.
http://www.apacs.org.uk/resources_publications/documents/annsumm06.pdf (obtained on 08/02/2007)
[2] Arora Anu, *Electronic Banking and the Law*, 3rded, IBC Business Publishing, London, 1997, at pp. 1-2.

context of EFT, to determine whether the payment order is an authorised payment order or not. Furthermore, section 1.2.5 focuses on the problem of identity authentication, which arises as result of sending payment orders by electronic means. A subsequent chapter will demonstrate that the application of the rules of agency law to fraudulent EFT is inappropriate and inadequate in dealing with the problem of identity authentication.

## 1.2.OVERVIEW OF INTERNATIONAL WHOLESALE ELECTRONIC FUNDS TRANSFER (EFT)

### 1.2.1. Synopsis of EFT

The starting point for any work on EFT is to define EFT, since the scope of the discussion in this thesis will depend heavily on such a definition. Electronic funds transfer means substituting paper-based payment instructions by electronic methods to authorise a financial institution to credit or debit account. [3] Geva states

> "[A] payment order is given electronically whenever it is embodied in a cable or telex ("wire"), initiated through a magnetic tape or diskette that may physically be delivered, or sent from a terminal over a dedicated communication network. Communication by wire or over dedicated network is on-line; when transmission immediately follows input it is also real time. An electronic funds transfer ("EFT") occurs whenever a payment order is given by any electronic means." [4]

In England, the Jack Committee Report defines EFT as

> "...payment messages transmitted either through magnetic material such as magnetic taps, disks, and cassettes; or through purely electronic media such as

[3] ibid at p.1.
[4] Benjamin Geva, "International Funds Transfers: Mechanisms and Laws," Chris Reed, Ian Walden, and Laura Edgar, (eds), *Cross-Border Electronic Banking, Challenges and Opportunities* 2nd ed, Published Jointly with The Centre For Commercial Law studies, Lloyd's of London Press, 2000 at p.6.

> telephones, telex, and electronic transmission between computers, or between a terminal and a computer." [5]

Accordingly, the difference between paper-based funds transfer and EFT is the method used to initiate the payment order. The EFT transaction occurs when the payment order to transfer money is initiated by electronic means. The payment order could be initiated by using off-line or on-line electronic means. [6] The Jack Committee Report states

> "[O]FF-LINE. Describes payment system which is not linked to a central computer where the data must be physically transmitted at the end of the day by tape, disc etc. Hence ON-LINE, which describe payment systems directly linked to a central computer and so capable of immediate account updating" [7]

An on-line means could for instance, be a closed network (dedicated network) [8] and an open network such as the Internet. [9] Both the open and closed networks fall within the scope of this thesis. A closed or dedicated network is defined as "[A] data communications network that is used for specific purpose, such as a payment system, and to which access is restricted." [10] In a closed network, only the bank's customer can access the bank's system through a dial-in or cable TV connection. [11] Moreover, in a closed network, access to the bank's systems is restricted to specific areas, therefore the customer cannot contact the bank's system wherever he goes in the world. [12] By contrast, an open network is " [A] data communication network to which

---

[5] Review Committee on Banking Services: law and practice, report by the Review Committee / Chairman: R.B. Jack, Vol. XLIX 622-630, 1989 at p. 75. (hereafter Jack Committee Report)
[6] Geva 2000, note 4 supra at p.6.
[7] Jack Committee Report, note 5 supra at p. X.
[8] Geva 2000, note 4 supra at p.6.
[9] Internet Banking: Comptroller's Handbook, Comptroller of the currency Administrator of national banks, (hereafter Internet Banking Comptroller's Handbook) October 1999 at pp.1 & 4. http://www.occ.treas.gov/handbook/intbank.pdf http://www.occ.treas.gov (obtained 25/4/2004).
[10] ibid at p.67.
[11] ibid at p.2.
[12] ibid.

access is not restricted." [13] In an open network, the customer can access the bank services through the bank's web site over the Internet. [14] The bank's web site provides the customer with information about the bank's services and/ or access to the bank services, so the customer can send payment order to his bank to transfer funds over the Internet. [15] Accordingly, Internet banking is defined as follows "[S]ystems that enable bank customers to access accounts and general information on bank product services through a personal computer (PC) or intelligent device." [16] The Internet banking services currently available for customers to use can be classified into three types. The first type of Internet banking is the "Informational" [17] type. This type of Internet banking provides customers with information about the bank services and products, and the customer cannot communicate with bank or make payment orders. [18] The second type of Internet banking is the "Communicative" type. [19] This type of Internet banking is more advanced than the former, as it enables the customer to communicate with his bank. [20] However, the customer is unable to send payment orders to transfer funds through such Internet banking services. [21] The communications between the bank and his customer may take the form of observing the account balance, applying for a loan, and requesting further information about specific bank services or products. [22] The third type of Internet banking is the "Transactional" [23] type. This type of Internet banking is the most advanced level of Internet banking service, because it enables the customer to access his account in

---

[13] ibid at p.78.
[14] ibid at pp. 2 & 90.
[15] ibid.
[16] ibid at p. 1.
[17] ibid at p. 4.
[18] ibid and Abu Bakar Munir, *Internet Banking: Law and Practice*, LexisNexis, London, 2004 at p 5.
[19] Internet Banking Comptroller's Handbook , note 9 supra at p.4
[20] Internet Banking Comptroller's Handbook ,ibid and Munir, note 18 supra at p.5.
[21] ibid.
[22] ibid.
[23] Internet Banking: Comptroller's Handbook ,ibid at p.5.

order to carry out transactions such as sending payment orders to transfer funds from one's own account to another and bill payments. [24] This thesis focuses on the "Transactional" type of Internet banking, as it enables the customer to carry out international wholesale EFT. Thereby, the definition of Internet banking in this thesis is a connection established between the customer's computer and the banking system via the bank's web site, which enables the customer to send payment order to his bank, where the customer has bank account, to debit the customer's account and credit the beneficiaries' account. [25]

Moreover, EFT, in this thesis, means a fund transfer carried out through the banking system by electronic means pursuant to an electronic payment order. The payment order is initiated by the customer by using on-line electronic means. According to this definition, all the steps of the payment process, including its initiation, must be executed by using on-line electronic means through either open or closed network. The definition adopted for this thesis stems from the fact that the arrival of the Internet has encouraged customers, banks and financial institutions to move from the traditional and off-line methods for money transfers and shift to on-line means. [26] Internet or on-line connections enable the customers to make their transactions with banks from their office (customers' office), [27] and the Internet enables the bank's customers to access their accounts to transfer money wherever they are in the world.[28] In 2006, the Yearbook of Payment Statistics of the Association for Payment Clearing

[24] ibid and Munir, note 18 supra at p.5.
[25] Internet Banking: Comptroller's Handbook ,ibid at p.1.
[26] ibid at p. 3 and Munir, note 18 pp. 9-11.
[27] Norbert Horn, *Legal Issues in Electronic Banking*, Kluwer Law International, The Hague; London 2002 at p. 4 and Munir, ibid.
[28] Internet Banking Comptroller's Handbook, note 9 supra at p. 2.

Services [29] (APACS) in UK demonstrated that in 2006, the use of cheques as a payment method in business transactions decreased by 4.7% in comparison to the year 2005. This figure shows that in 2006, the volume of cheques used in business transactions was 585 million, in comparison to 613 million volumes of cheques used in the previous year. By contrast, in 2006 the same statistics shows 5.4% a considerable increase in the percentage of automated payments used in business transactions. This figure shows that in 2006, the volume of automated payments used in business transactions was 301 million, in comparison to 286 million volumes of cheques used in 2005. [30]

Equally important, this thesis is devoted to on-line EFT, because on-line methods of transfer funds give rise to two main legal problems, which are less problematic in off-line means. These two main problems are the problem of identity authentication and the problem of an authenticated but unauthorised payment orders. [31] These problems are more obvious and significant in on-line means than in off-line means because with on-line means a large amount of funds transfer could be transferred instantly over open or closed networks which are probably vulnerable to interception by a third party.

[29] APACS was established in 1985. The three major clearing systems companies in UK are working under the auspices of the APACS. The first system is paper-based system is known as the cheque and credit clearing system run by the Cheque and Credit Clearing Co Ltd. The second system is electronic payment system is the CHAPS Sterling and Euro run by the CHAPS Clearing Co Ltd. The third system is also electronic payment system is known as BACS run by the Banker's Automated Clearing Services Ltd. Association for Payment Clearing Services Yearbook of UK Payment Statistics May, 2004, pp. 8-9.

[30] Association for Payment Clearing Services, Yearbook of UK Payment Statistics, p.80.

[31] See section 1.2.5 of this chapter for more details.

## 1.2.2. Legal Concept of International Wholesale EFT

EFT is classified as a credit or debit transfer. [32] In a debit transfer the beneficiary instructs his bank to collect money from the originator, whereas, in a credit transfer, the originator instructs his bank to debit his account and credits the beneficiary's account at the same bank or another bank. [33] Moreover, EFT may be used in wholesale movement of funds between banks, between banks and financial institutions or major corporate customers or in retail consumer transactions. [34] The focus of this thesis is on wholesale EFT. Alternatively, electronic funds transfer could be classified to "non-consumer activated EFT systems" and "consumer-activated EFT system." [35] The wholesale transactions or "non-consumer activated EFT systems" transactions are executed through large value payment systems (CHIPS, FEDWIRE, CHAPS and TRAGET) or SWIFT, while the retail transactions or "consumer-activated EFT system" are executed through ATMs, credit and debit cards. [36] Retail consumer transactions in some countries are governed by a specific legislation that regulates the bank-customer relationship. For example, in England the Consumer Credit Act 1977 and Unfair Terms in Consumer Contracts Regulations 1999 (hereafter UTCCR) govern retail transactions. [37] In the US, the Electronic Funds Transfer Act 1978 governs retail transactions. [38] A retail consumer transaction such

---

[32] Geva 2000, note 4 supra at p.2 and E. Ellinger, Eva Lomnicka and Richard Hooley, *Ellineger's Modern Banking Law* 4th ed, Oxford University Press, New York, 2005 at p. 515.
[33] Geva 2000, ibid and Ellinger, Lomnicka and Hooley, ibid.
[34] Jack Committee Report, note 5 supra at p. xi.
[35] Mark Hapgood, QC, *Paget's Law of Banking* 12thed, Butterworths, London 2002 at p. 286.
[36] ibid.
[37] Ahmed Azzouni, "Internet banking and the Law: a critical examination of the Legal controls over Internet banking in the UK and their ability to frame, Regulate and secure banking on the net," J.I.B.L.R. 2003, 18(9), 351-362 at p.361.
[38] Chris Reed, "Consumer Electronic Banking," Chris Reed, Ian Walden, and Laura Edgar, (eds), *Cross-Border Electronic Banking, Challenges and Opportunities*, 2nded, Published Jointly with The Centre For Commercial Law studies, Lloyd's of London Press, 2000 at p.162.

as involving debit and credit cards is used to pay for goods and services by transferring the money electronically from the customer's account to the retailer's account. [39] Thus, a retail transaction contains different relationships and every relationship is governed by separate contract. Firstly, there is a contract between the customer (the payer) and the customer's bank (the paying bank), Secondly, there is a contract between the retailer (beneficiary) and the retailer's bank (the beneficiary's bank). Thirdly, there is a contract between the customer (the payer) and the retailer the (beneficiary) and lastly, there is a contract between all the banks and the financial institutions involved in retail transactions. [40] Furthermore, retail consumer transaction can be executed over the counter, via telephone and the Internet. In the UK, statistics show that losses as a result of card fraud overall have declined by 5% in the first six months of 2006. However, the figures show that the losses as a result of card fraud when the card details were transmitted over the internet, telephone or mail order have risen to £ 95.3 million in the first six months of 2006 in comparison to £90.6 million in the first six months of 2005 and 70.2 million in the first six months of 2004. [41]

International wholesale fund transfers are always credit transfers. [42] In credit transfers, the payer is called the originator, and the payer's bank the originator's bank, whereas the payee is called the beneficiary and the payee's bank the beneficiary's

---

[39] David Robinson, " The structure and Characteristics of the Principal Electronic Banking systems," Royston Goode (ed), *Electronic Banking: The Legal Implications,* Institute of Bankers, London, 1985 at p.1.

[40] Arora 1997, note 2 supra at pp.44-46.

[41] APACS the UK Payments Association, Press Releases, "Latest Figures Show UK Card Fraud Losses Continue to Decline in First Six Months if 2006," 07/11/2006. (hereafter APACS press releases 2006) http://www.apacs.org.uk/media_centre/press/06_07_11.html (obtained on 09/02/2007).
"Chip and PIN Sends Card Fraud Online in the UK," Out-Law News, 08/11/2005.
http://www.out-law.com/page-6315
http://www.out-law.com (obtained on12/12/2005).
"Chip and PIN Sends Card Fraud Online in the UK," Out-Law News, 08/11/2005.
http://www.out-law.com/page-6315
http://www.out-law.com (obtained on12/12/2005).

[42] Hapgood, note 35 supra at p.300 and Ellinger, Lomnicka and Hooley, note 32 supra at p. 520.

bank. The participating banks in the transaction other than the originator's bank and the beneficiary's bank are called intermediary banks. [43] In credit transfers, the originator instructs the originator's bank to debit his account with a specific amount of money to credit the beneficiary's account. [44] According to Article 2 (a) of the UNCITRAL Model Law, a credit transfer [45] means a

> "[S]eries of operations, [successive bilateral credit transfers] [46] beginning with the originator's payment order, made for the purpose of placing funds at the disposal of a beneficiary. The term includes any payment order issued by the originator's bank or any intermediary bank intended to carry out the originator's payment order. A payment order issued for the purpose of effecting payment for such an order is considered to be a part of a different credit transfer."

Indeed, the same meaning of credit transfer has been adopted in s.104 (a) of Article 4A and Article 2 (f) of the EU Directive. As a result, UK Regulations have adopted the same meaning. These Regulations define cross-border credit transfer as

> "[A] transaction or series of transactions carried out as a result of instructions given directly by an originator to an institution in one EEA State, the purpose of which is to make funds in an EEA currency available to a beneficiary at an institution in another EEA State; and for the purposes of this definition the originator and the beneficiary may be one and the same person." [47]

An international credit transfer occurs when the originator's bank and the beneficiary's bank are in different countries, regardless of the customers' location. According to Article 1 (1) of the UNCITRAL Model Law, "this law applies to credit transfer where any sending bank and its receiving bank are in different states."

---

[43] Article 4A of Uniform Commercial Code 1989, s. 4A-103 (a) (2) (3)
Article 4A of the Uniform Commercial Law 1989.
http://www.law.cornell.edu/ucc/4A/ (obtained 08/02/07)
http://www.ali.org/
and s. 4A-104 (b) (c) (d), the UNCITRAL Model Law, art. 2 ,Benjamin Geva, *Bank Collections and Payment Transactions, Comparative Study of Legal Aspects*, Oxford, New York: Oxford University Press, 2001, at pp.212& 393 and Ellinger, Lomnicka and Hooley, note 32 supra at p.514 and Geva 2000, note 4 supra at p.3

[44] Geva 2001, ibid at p.187, Ellinger, Lomnicka and Hooley, note 32 supra at p.515 and Geva 2000, note 4 supra at p.3.

[45] See the Uniform Commercial Code 1989, Article 4A-104 for definition of credit transfer.

[46] Words in square brackets added.

[47] UK Cross-Border Credit Transfer Regulations 1999/ No.1876, reg 2 (b).

Moreover, the EU Directive [48] and the UK Regulations, [49] apply to credit transfer executed between different banks in different Member States, regardless of the customers' location. On the other hand, national credit transfers take place when the originator's bank and the beneficiary's bank are in the same country. This thesis is confined to international EFT as it is more related to wholesale EFT than national EFT. In fact, wholesale funds transfers are mostly used to settle international funds transactions, which are often carried out, by intermediary banks. It is worth noting that the relationship between the originator and the originator's bank, which is the focus of this thesis, is a national relationship. As in such a case, the business customer issues a domestic payment order to his bank in the same country to transfer funds to the beneficiary's bank account in a different country. Geva states that

> "[A]n international funds transfer occurs where either the originator's bank or the beneficiary's bank, or both banks are located in a country other than that of the currency of the transfer. A cross-border overseas bank is considered as a separate bank for these purposes." [50]

In regards to funds transfer between Member States of the single European currency, the relation between the currency and the country is irrelevant in determining whether a funds transfer is a cross-border credit transfer or not. According to the EU Directive cross-border credit transfer is a funds transfer executed between different banks located in different Member States, regardless of the currency used in the transaction. It is worth noting that UK is not a member of a single European currency.

Indeed, international credit transfer may be "correspondent" or "complex." [51] A correspondent credit transfer happens when the originator and the beneficiary hold accounts in different banks, and one of the banks holds an account with the other

---

[48] The Council Directive 97/5 on Cross-Border Credit Transfer, February 14, 1997 OJ L 43 at P. 0025 – 0030 1997, art. 1.
[49] UK Cross-Border Credit Transfer Regulations 1999 reg. 2 (b).
[50] Geva 2001, note 43 supra at p.188.
[51] ibid 187.

bank. [52] For example, if the originator has account with X bank and the beneficiary has account with Y bank, either X bank should hold an account with Y bank, or Y bank should hold an account with X bank. In this case, the settlement between the two banks will be executed on the books of the bank that has the account of the other bank. This occurs either by debiting the originator's bank account and crediting the beneficiary's account or debiting the originator's account and crediting the beneficiary's bank account. A complex credit transfer means that an intermediary bank has bilateral, correspondent relationship with the two banks. Where the two banks hold an account in the same bank, in such cases this bank will act as an intermediary bank by debiting the originator's bank account and crediting the beneficiary's bank account. [53]

In international credit transfer, the originator's bank according to the originator's instruction (payment order) debits the originator's account and sends the payment order to the receiving bank; the receiving bank could be an intermediary bank or the beneficiary's bank. [54] If the payment order has been sent to an intermediary bank, the intermediary bank will send the payment order to the other intermediary bank or the beneficiary's bank. Many payment orders may be issued several times in the same credit transfer transaction, until the beneficiary's bank credits the beneficiary's account.[55] Therefore, with an international credit transfer, often more than one intermediary bank is involved in the transaction. A settlement is not directly possible between the originator's bank and the beneficiary's bank, as banks do not have branches all over the world, and cannot maintain a correspondent relationship with all

[52] ibid.
[53] ibid 188.
[54] Geva 2000, note 4 supra at p. 3.
[55] ibid.

other banks or a shared correspondent bank with others banks. [56] Therefore, a transaction could involve several intermediary banks, each executing the payment order it receives from the preceding bank by issuing, in turn, a payment order to the next bank in the funds transfer chain. Each intermediary bank generates a new payment order and a new settlement.

Finally, the credit transfer could be accomplished through a Clearing House for netting and settlement. A settlement can be made on the books of a central counterparty, with whom all the banks holds account such as central bank. [57] In such circumstances, the originator's bank instructs a local bank in the country of the currency to credit the beneficiary's account at the beneficiary's bank. Consequently, the local bank will transfer the money to the beneficiary's bank through the local clearing payment systems, for instance, CHAPS or CHIPS. [58]

### 1.2.3. Why this Thesis Focuses on Fraudulent EFT's.

The scope of this thesis examination is confined to fraudulent international wholesale EFT, for the following reasons. Firstly, fraudulent international wholesale EFT has been a topic that has given rise to heated legal debate between banks, customer's representatives and many international organisations. [59] This debate is justified on the basis that international wholesale EFT involves huge sum of money and disruption of

---

[56] Geva 2001, note 43 supra at p.194.
[57] ibid.
[58] ibid.
[59] Gregor G. Heinrich, "Funds Transfer, Payments and payment Systems-International Initiatives Towards Legal Harmonisation," Norton Joseph, Chris Reed and Ian Walden, (eds), *Cross-Border Electronic Banking, Challenges and Opportunities*, Published Jointly with The Centre For Commercial Law studies, Lloyd's of London Press, 1995 at pp. 233-265, Jack Committee Report, note 5 supra and UNCITRAL, Model Law on International Credit Transfers: compilation of comments by Governments and international organizations (A/CN.9/347 and Add.1) [page 102]. http://www.uncitral.org/english/yearbooks/yb-1991-e/vol22-p102-144-e.pdfindex.htm http://www.uncitral.org (obtained on 22/6/2004).

such transactions by fraudulent acts has a significant effect on the financial markets, the banks and the business customers. [60] The absence of particular rules devoted to EFT gives rise to a significant debate in the context of the parties' rights, duties and liabilities for EFT and particular fraudulent EFT. [61] Bhala aptly argues that

> " [W]ith so much money transferred by wire each day, and with the average value of each transfer so high, the potential for large losses is great. Thus, institution sending and receiving such payments require a clear, comprehensible, and sensible legal regime to answer two basic questions. First, how should a wire transfer normally work? Second, what happens if mishap occurs? There is a third public policy issue of particular concern to central bankers, namely, systemic risk - how can this risk be minimized and contained?" [62]

Bhala has explained that when banks and their customers who participate in wholesale EFT cannot predict their rights, duties and liabilities when "mishap occurs", such as fraud they will be reluctant to use wholesale funds transfer as a mean of transferring money.[63] Moreover, as a result of uncertainty and unpredictability, the banks will be reluctant to execute EFT at high speed and low cost. [64] Since EFT is used to accomplish huge financial transactions between financial institutions in different financial markets in variant countries such as, foreign exchange trade and derivatives transactions. [65] Consequently, the financial markets' operations and functions will be hindered and this may affect the world economy. [66] Accordingly, this thesis will

---

[60] Raj Bhala, " International Payments and Five Foundations of Wire Transfer Law," Essays in International Financial & Economic Law No, 2, International Finance and Tax Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, University of London, in cooperation with the London Centre for International Banking Studies and the London Institute of International Banking, Finance and Development Law, London, 1996 at p.6.
[61] Luc Thevenoz,, "Error and Fraud in Wholesale Funds Transfers: U.C.C. Article 4A and The UNCITRAL Harmonization Process," 42 Ala. L. Rev.881, Winter, 1991 at pp.882-883.
[62] Bhala, note 60 supra at p. 7.
[63] ibid.
[64] ibid.
[65] ibid at p.6 and Richard Dale, " Controlling Risks in Large Value Interbank Payment Systems," J.I.B.L. 1997,12(11), 426-434 at p. 426.
[66] Bhala ibid at p. 7 and Razeen Sappideen, "Cross-Border Electronic Funds Transfers through Large Value Transfers Systems and the Persistence of Risk," 2003, J.B.L., pp.584-602 at p. 584.

examine the bank-customer's rights, duties and liabilities for fraudulent international wholesale EFT under the UK law, EU law, US law and the UNCITRAL Model law.

Secondly, in the UK, a paramount step should be taken to enact rules determine the bank and the customer's rights, duties and liabilities for fraudulent EFT, as the statistics shows that losses of online banking fraud have risen by 55% to £22.5 million in the first six month of 2006 in comparison to £14.5 million on the first six months of 2005, whereas, in the first six months of 2004 the losses of online fraud banking were £14.5 million. [67] However, apart from the UK regulations that apply to EFT up 50,000 Euros, in England there is a consensus that there is no "comprehensive statutory regime," [68] to regulate wholesale EFT valued at more than 50,000 Euros. [69] Furthermore, the UK regulations do not cover all the problems that may arise in the context of EFT such as fraud. [70] Instead, EFT valued at more than 50,000 Euros are regulated by the general principles and rules of contract law, agency or mandate law and by analogy with the rules that apply to forged cheques. [71] Baker and Brandel have rightly stated that there are inherent major risks that exist in international EFT such as fraud, error, system malfunction and the insolvency of the receiving bank. [72] Therefore, given the above figures and the absence of a "comprehensive statutory regime" may give rise to the following problems. The first problem is the distribution of liability for fraudulent EFT between the originator and the originator's bank. When

---

[67] APACS press releases 2006, note 41 supra.
[68] Ellinger, Lomnicka and Hooley, note 32 supra at p. 543, Hapgood, note 35 supra at p.330 he used the term "all-embracing statutory regime" and Richard Hooley and John Taylor, "Payment By Funds Transfer," Michael Q.C. Brindle and Raymond Cox, (eds) 3rd ed, *Law of Bank Payments*, Sweet & Maxwell, London 2004 at p. 107.
[69] Geva, 2001 note 43 supra at p.212, 393, Ellinger, Lomnicka and Hooley, note 32 supra at p.492 and Hapgood, note 35 supra at p.330.
[70] Arora, Anu, " Round up: Banking Law," Comp. Law. 2000, 21(8), 234-244, at p. 244.
[71] Arora 2000, ibid, Geva 2001, note 43 supra at p.212, 393, Ellinger, Lomnicka and Hooley, note 32 supra at p.492 and Hapgood, note 35 supra at p.330.
[72] Donald I. Baker and Roland E. Brandel, *The Law of Electronic Fund Transfer Systems: Legal and Strategic Planning* revised edition, Warren, Gorham & Lamont, Boston 1996 at pp.30-11.

an EFT is executed fraudulently by one of the originator's bank employees, or the originator's employees or by a third party. Smart has argued that applying mandate rules to the bank-customer relationship in the context of EFT poses a number of questions: [73] for instance, the allocation of liability between the bank and the customer in case of fraud and error in EFT [74] and the legal validity of the PIN to replace the handwritten signature. [75] Subsequent chapters will demonstrate how applying the law of mandate raises the problem of liability allocation, as applying mandate rules make the parties' liabilities unpredictable and uncertain. Moreover, the validity of the PIN in the context of EFT under the English law will be discussed in Chapter two. Chapter two will demonstrate that in England the validity of the PIN or any other type of security procedures such as E-signature does not pose a problem currently. [76] As all type of security procedures are currently valid according to the recent case law, [77] and after the adoption of Electronic Communications Act 2000 and E-Signature Regulations 2002. However, these legalisations are not helpful to determine the legal effect of the security of procedures on the originator and the originator's bank's liability for fraudulent EFT.

The second problem that may arise in the absence of "comprehensive statutory regime" is the scope of the originator and the originator's bank's liability for direct damages and consequential damages occurred as a result of fraudulent EFT. The third problem that may arise is the absence of "comprehensive statutory regime", with EFT the bank receiving the payment order form its customer through electronic means,

---

[73] Eynon Smart, "Electronic Banking: An Overview of the Legal Implications," Royston Goode, *Electronic Banking: The Legal Implications,* Institute of Bankers, London 1985 at p.2.
[74] ibid.
[75] ibid 3.
[76] Chris Reed, "What is a Signature?" (JILT), Issue 3, 2000. http://elj.warwick.ac.uk/jilt/00-3/reed.html/
[77] *Goodman v. J Eban Ltd,* [1954] 1 Q.B. 550.

without face-to-face interaction. The absence of face-to face communication gives rise to significant legal problem, the problem of identity authentication and how the bank can determine whether the payment order is an authorised payment order or not. Azzouni has argued that in England the legal issues related to Internet banking such as error, fraud, security procedures and the liability of the parties in the context of funds transfer have been left without persuasive answers. [78] Azzouni has rightly argued that the reason for that is implementation of the existing laws to Internet banking in particular agency law, contract law and the rules apply to forged cheques lead to unpredictability and uncertainty of the liability allocation for unauthorised funds transfer transactions. [79] Azzouni justified his view, which the present author agrees by the following:

> "[T]he discussion of the different types of services, security, privacy and other legal issues, reveals that there are still many uncertainties regarding most aspects of online banking. The diversity in interpreting legal provision and the different decision held in cases with identical facts is another example of the incapability of the traditional law to deal with the distinct nature of the Internet. Furthermore, in the absence of regulations dealing with specific issues of Internet banking, such as liability, banks draw these rules trying to achieve the minimum liability in cases of system malfunctions and fraudulent transactions." [80]

Furthermore, the present author's view is that the unpredictability and uncertainty existing in that the parties cannot decide when they would be found liable for authenticated but unauthorised payment order. Moreover, the parties are unable to predict and cannot know for certain the limits of their liabilities for direct and consequential damages in addition to interest.

The last problem that may arise in the absence of "comprehensive statutory regime" is whether the standard of security procedures implemented by the banks are reasonable

---

[78] Azzouni, note 37 supra at p. 351.
[79] ibid 362.
[80] ibid.

and acceptable to the customer. The security procedures used to protect the banks and the customers' communications are implemented by the banks, and in the account agreement, the banks tend to exclude their liability for fraudulent EFT executed by third party who manages to by pass such procedures. Accordingly, rules are needed to determine the reasonable standard of security procedures should be implement by the bank to protect the customer's account from fraudulent EFT executed by third party. Furthermore, whether depending on such security procedure the bank can escape liability for fraudulent EFT. This thesis, in subsequent chapters, will demonstrate that in the absence of rules regulate and determine the standard of security procedures should be implemented by the bank. Banks under contract law are able to escape liability for EFT executed fraudulently by a third party by passes the security procedures by incorporating exclusion term in the account agreement.

Thirdly, in 1989, the Jack Committee Report on Banking Services: Law and Practice (hereafter Jack Committee Report) discussed the issues related to EFT, for example the need for regulations to govern and regulate EFT legal problems which arise as a result of using the communication technology for issuing the payment order. [81] These problems are the authenticity of payment orders, the standard of security procedures and the loss allocation between the bank and its customer in case of fraud and error. However, the Jack Committee Report dealt with retail EFT (fraud in credit card), but the Report recognized and acknowledged that the above-mentioned legal problems are "intrinsic to the nature of EFT," despite of the type of funds transfer. [82] Equally important, the Jack Committee Report recommended that new rules for retail EFT were needed, and such problems should not be left to contractual arrangements to

[81] Jack Committee Report, note 5 supra, at pp.77-81.
[82] ibid at p. 77.

solve them. [83] By analogy, the problems of authenticity of payment orders, the standard of security procedures and the loss allocation between the bank and its customer arise in the context of fraudulent wholesale EFT should not be left to contractual arrangements to be solved. Bhala aptly confirmed that:

> "[I]t is not overstatement to say that wire transfers are the most significant cross-border payment mechanism. First, because they are used to settle financial market transactions – foreign exchange trade, derivatives transactions, etc. – they are the backbone of international financial markets. Second, because of huge amount funds transferred by wire they demand special attention." [84]

Fourthly, in England, large value funds transfers have been given less attention in academic writing and legislation than small value funds transfer. One of the reasons for this is that the bank and the customers in wholesale EFT acquire equal bargaining powers, so both of them are able to negotiate the contract terms, and the business customers acquire the power to reject unfair contract terms. However, not all customer business has equal bargaining power to negotiate the terms of the contracts in particular small and medium-sized corporations. [85] Therefore, some of business customers still need to be protected against unfair contract terms. This thesis will demonstrate that bank account agreements and contract law does not alleviate the uncertainty and unpredictability of parties' rights, duties and liability in the context of fraudulent wholesale EFT. Thevenoz states

> "[W]hy would bankers and their counsels, who usually favor contractual solutions to legislative solutions, concur with their corporate clients in supporting the codification of "the web of laws that has traditionally governed the conduct of parties to international payments"? The absence of well-defined body law applicable specifically to paperless funds transfer, both in Common Law and in several Civil Law countries, has created much uncertainty, especially with regard to the finality and revocability of a payment order, and the allocation of losses in case of fraud, error and insolvency. These uncertainties became a major concern to banks experiencing the lack of a

[83] ibid at p. 81.
[84] Bhala, note 60 supra, at p.6
[85] Geva 2001, note 43 supra at p. 29.

> statutory "safety net" as soon as some of their largest clients refused to accept disputed contractual provisions allocating losses." [86]

Fifthly, in England, the payment system that transfers the greatest value of money between different parties is governed by general principle of different sources of law such as contract law, agency law and the rules apply to forged cheques. In contrast, other payment systems such as cheques and credit cards are governed by a comprehensive body of statutory law. For instance, the Bill of Exchange Act 1882, the Consumer Credit Act 1974, Unfair Terms in Consumer Contracts Regulations 1999 (hereafter UTCCR) and UK Regulations. Bhala has affirmed that given the large amount of money transfers via wholesale EFT, there is a need for "sensible legal regime" to regulate wholesale EFT. [87]

Ahn argues that

> "[T]he price-and time-sensitive nature of funds transfers as a mode of payment demands a high degree of certainty and predictability—the parties involved in such transactions must be able to anticipate and minimize these liabilities, or if they cannot, at least be able to predict with some confidence on who the liabilities will fall." [88]

The present author will demonstrate and argue in subsequent chapters that applying the general principles of contract law, agency law and the rules apply to forged cheques are not effective in regulating and governing problems arising in the context of fraudulent EFT. These problems are the parties' liability for authenticated but unauthorised payment orders, their liability for direct and consequential damages, and unfair contract terms that the bank includes in its contracts.

Lastly, in England, there is lack of case law in the context of fraudulent EFT. The lack of case law might show that banks are very keen to solve the problem of

---

[86] Thevenoz,, note 61 supra at pp.882-883.
[87] Bhala, note 60 supra at p.7.
[88] Hyung J. Ahn, " Note Article 4A of the Uniform Commercial Code: Dangers of Departing from a Rule of Exclusivity," 85 Va. L. Rev. 183, Feb 1999 at p. 186.

fraudulent EFT without going to court, [89] as bringing action against the bank for fraudulent EFT may affect the bank's reputation and reliability to provide EFT services to its customer. Therefore, the aim of this thesis is to assist in applying the general principles of contract law, agency law and the rules that apply to forged cheques to fraudulent EFT. Subsequently, this thesis will demonstrate that applying the former rules to fraudulent EFT does not alleviate the unpredictability and uncertainty in the customer-bank's rights, duties and liabilities in the context of fraudulent EFT.

EFT gives rise to significant legal relationships between firstly, the originator and the originator's bank, secondly, the originator's bank and the intermediary bank, thirdly, the originator and the intermediary bank and lastly, the beneficiary and the beneficiary's bank. Whilst the present author appreciates the significance of all the above-mentioned relationships. The particular focus of this thesis is to examine the legal relationship between the originator and the originator's bank in the context of fraudulent EFT under contract and agency English common law, the UK regulations, the EU Directive, Article 4A and the UNCITRAL Model Law. The participant banks in EFT are members in payment systems such as CHIPS, CHAPS and TARGET. [90] The relationship between originator's bank, the intermediary bank and the

[89] Sam Coats and Joe Morgan, "Victims of Internet Bank Fraud Will have to Pay up," The Times, Saturday, Nov, 13, 2004, p.14.

[90] Ellinger, Lomnicka and Hooley, note 32 supra at pp. 521-522, 532-537 and "Payment Systems in Euro Area," Bank on International Settlement, CPSS-Red-Book,2003.
http://www.bis.org/cpss/paysys/ECBComp.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp-o=2,100000,0
http://www.bis.org/index.htm (obtained 3/2/2004).
"Current Topics in Payment and Settlement Systems," Committee on Payment and Settlement System (BIS), Dec,1999.
http://www.bis.org/publ/cpss35.pdf
http://www.bis.org/index.htm (obtained 3/2/2004).
"CHIPS Rules and Administrative Procedures," November 2003.
http://www.chips.org/infofiles/CHIPS_rules.pdf
http://www.chips.org (obtained 3/2/2004).

beneficiary's is already sufficiently regulated and does not give rise to significant problems. The reason for that is every participant in the payment systems signed a contract provides that the participant is bound by the payment systems rule.[91] According to such a contract, the participant has a contractual relationship with the payment system and with other participants in the payment system. [92] The payment system's rules determine the parties' rights, duties and liabilities against each other and the payment system. For instance, Rule 16 of CHIPS governs the participant's liability for a payment order that has been executed fraudulently and Rule 7 determines the standard of security procedures should be implemented by the participants. [93] Thus, the participants' rights, duties and liabilities for fraudulent EFT are predictable and certain, as they are determined by the payment system's rules.

By contrast, the payment systems' rules do not govern and regulate the relationship between the originator's bank and the originator. [94] Likewise, the payment system's rules do not determine which party is liable for fraudulent EFT and whether the originator's bank is liable for consequential damages against the originator. [95] Equally important; the participant banks in EFT have equal bargaining power, but the bargaining powers between the originator and the originator's bank is not always equal, and the originator needs protection against unfair contract terms in the context of fraudulent EFT. Geva confirms

> "[I]n all jurisdictions, the account agreement consists of express as well as implied terms. The latter may partly be customary or usage based. The former are typically standard form contracts, which as a rule, tend to favour the bank. This is so not only vis-à-vis small customers, particularly consumers, but

[91] Hooley and Taylor, note 68 supra, at p.101.
[92] ibid
[93] CHIPS Rules, note 90 supra at pp. 5 & 23.
[94] Ernest T. Patrikis, Raj K. Bhala and Micheal T. Fois, "An Overview of United States Funds Transfer Law," Robert C. Effros (ed), *Payment Systems of the World*, Oceana Publications, New York, London, 1996 at pp. 5-6.
[95] ibid.

potentially, also towards large corporate customers, which by nature of things, deal with the bank not in the context of their main line of business. As such, terms in account agreement are characteristically narrowly construed against the bank." [96]

This thesis will demonstrate that the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT need to be regulated by rules devoted to EFT, as the rules of contract law lead to unpredictability and uncertainty.

## 1.2.4. DEFINING FRAUDULENT EFT IN ENGLISH LAW

### (a) Concept of Fraud in the Context of EFT

In 2004, because on-line attacks against on-line accounts have risen suddenly in the United Kingdom, banks have decided not to pay the debts of victims of Internet fraud.[97] In the first half of 2004, banks paid more than £4.5 million for 2000 customers (fraud victims). [98] Banks paid compensation directly to the victims themselves, as they are not insured against losses. [99] The parties' liability for fraudulent EFT affects the cost, speed and security of EFT services which makes the issue of liability for fraudulent EFT of concern for both banks and customers.

Ulph believes that Kirk's definition of fraud could be applied to fraud in context of commercial civil law, Kirk defines fraud as "the dishonest non-violent obtaining of some financial advantage or causing of some financial loss." [100] However, in England, there is no statutory or common definition for fraud in general or for EFT fraud in

[96] Geva 2001, note 43 supra at p. 29.
[97] Coats and Morgan note 89 supra.
[98] ibid.
[99] ibid.
[100] Janet Ulph, *Commercial Fraud: Civil Liability, Human Rights, and Money Laundering,* Oxford University Press, 2006, at p.6 and Davis Kirk, "Serious Fraud- A Banker's Perspective," Joseph Norton (ed), *Banks Fraud and Crime,* Published Jointly with The Centre For Commercial Law studies, Lloyd's of London Press,1994 at p.11.

particular.[101] Goldspink and Cole have stated that "[E]nglish civil law has never sought to define the expression "fraud" or to provide a unified set of rules dealing with rights and remedies arising in respect of those whose conduct is generally described as fraudulent." [102] Therefore, the civil rights and remedies of fraud are taken from different legal sources. [103] This section aims to demonstrate how and when the act of fraud occurs in the context of EFT. In the absence of such a definition, as mentioned before, it is inevitable to consult and import from criminal law and case law. As Buckley J. in *Re London & Globe Finance Ltd* [104] has stated, fraud is defined as follows:

> " to deceive is, I apprehend, to induce a man to believe that a thing is true which is false, and which the person practising the deceit knows or believes to be false. To defraud is to deprive by deceit: it is by to induce a man to act to his injury. More tersely it may be put, that to deceive is by falsehood to induce a state of mind; to defraud is by deceit to induce a course of action." [105]

Accordingly, in terms of criminal law, fraud is a combination of two factors: theft and deception. [106] Moreover, Dawson has stated that according to Buckley J's judgments "that fraud must have two essential elements: deception or concealment; and deprivation or loss of victim." [107] After the Fraud Act 2006, which came into force on 15th January 2007 deception is no longer an essential element to establish fraud. [108] Deception offences under sections 15 and 16 of the Theft Act 1968 were replaced

---

[101] Ulph, ibid, Kirk, ibid, L.H Leigh, "Banks-Fraud and Crime: A Survey of Criminal Offences Under English Law," Joseph Norton (ed), *Banks Fraud and Crime*, Published Jointly with The Centre For Commercial Law studies, Lloyd's of London Press,1994 at p. 1-4 and Simon Dawson "Computer Fraud: Part 1: The Risk to Business," C.T.L.R.1999, 5 (3), 70-73 at p. 70.
[102] Robert Goldspink, and Jermey Cole, *International Commercial Fraud* 1st ed, Sweet and Maxwell, 2002at p. 2-01.
[103] ibid.
[104] *Re London & Globe Finance Ltd*, Chancery Division, [1903] 1 Ch. 728.
[105] ibid at pp. 732-733.
[106] Leigh, note 100 supra at pp. 1-4.
[107] Dawson, note 101 supra at p. 70.
[108] Fraud Act 2006, Chapter 35, section 1.

with three new fraud offences, according to section 1 of the fraud Act 2006, [109] namely, fraud by false representation, fraud by failing to disclose information and fraud by abuse of position. The Fraud Act 2006 does not define the concept of "fraud." Thus, Ormerod confirms that there is no common definition of "fraud" in common law. [110] According to section 2 of the Fraud Act 2006, fraud by false representation occurs when a person dishonestly makes a false representation of fact or law knowingly that the representation was or might be false. Moreover, the person who makes the representation intends to make a gain or cause loss for himself or another.[111] Section 2 (4) of the Fraud Act 2006 provides that false representation might be express and implied, traditionally such representation would be by word or conduct. [112] The Home Office explanatory notes on section 2 (4) demonstrates that "there is no limitation on the way in which the representation must be expressed. So it could be written or spoken or posted on a website." The representation under the fraud Act 2006 is wide enough to encompass the conduct of using somebody's credit card dishonestly without authority, and "phishing," where a person sends email to group of people asking them to provide their banks' account detail to gain access to their money. [113] One of the Fraud Act 2006 aims is to criminalize the new types of fraud executed by using the new types of communication technology which are used to accomplish financial transactions. [114] Therefore, section 2(5) of the Fraud Act 2006 devoted to criminalize the situations where the false representation submitted to one of the new types of communication technology. Such as "CHIP and PIN" machine,

---

[109] David Ormerod, "The Fraud Act 2006-Criminalising Lying," legislative Comment, Crim. L.R. 2007, Mar, 193-219, at pp.193-195.
[110] ibid, at p. 195.
[111] Ormerod, note 109 supra at p. 196.
[112] ibid, at p. 197 and Home Office Explanatory Notes on the Fraud Act 2006, note 14. (Hereafter Home Office Notes)
[113] ibid, Home Office Notes, note 15 and 16.
[114] Ormerod, note 109 supra at p. 195.

electronic systems and devices which are designed to accept and accomplish the order without human intervention. [115] Ormerod rightly argues that section 2 of the Fraud Act 2006 provides sufficient protection against electronic fraud. [116]

Accordingly, in the UK fraud in the context of EFT occurs whenever the former elements exist. In the context of EFT the false representation takes the form of getting unlawful or unauthorised access to originator's account. For instance, Internet "hackers" [117] attack the security procedures and gain unauthorised access to the originator's account by different methods such as "sniffers," [118] "Trojan Horse" [119] and "Hijacking." [120] By getting the unauthorised access the fraudster falsely representing to the originator's bank that he or she has the authority to send the payment order and to transfer money. The gain to the fraudster himself or to another and the loss of victim occurs when the originator's account is debited according to unauthorised payment order and the money transferred to a third party's account. According to section 5 (2) of the Fraud Act 2006 the terms " "[P]roperty" means any property whether real or personal (including things in action and other intangible property)." Consequently, a fraudulent act in the context of EFT falls within the ambit of the Fraud Act 2006, as an EFT payment order is a form of intangible property. Fraudulent EFT in the context of this thesis is an unauthorised payment

[115] ibid, at pp.199-200 and Home Office Notes, note 112 Supra, note 17.
[116] Ormerod, note 109 supra at. 200.
[117] Internet Banking Comptroller's Handbook, note 9 supra at p. 71 defines Hacker as "A computer operator who breaks into a computer without authorization, for malicious reasons, just to prove it can be done, or for other personal reasons.
[118] ibid, at p. 58 defines Sinffers as " Also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture log-on, Ids and Passwords."
[119] ibid, defines Trojan Horse as "A program can embed code into a system that will allow the program or another person unauthorised entrance into the system or network.
[120] ibid, defines Hijacking as "intercepting transmissions then attempting to deduce information from them. Internet traffic is particularly vulnerable to this threat.

order, [121] which occurs whenever the payment order is issued or altered by an unauthorised person to debit the originator's account, and to credit that amount of money to his account or any other account the unauthorised person may choose to direct the money for his account. [122] For instance, when the payment order is issued by firstly, one of the originator's bank employees, secondly, issued by one of the originator's employees who unauthorised to issue such payment order and lastly, issued by a third party.

**(b) Types of Fraud in the Context of EFT**

The subsequent chapters will demonstrate that originator and the originator's bank liability for fraudulent EFT is affected by the person who executes the fraudulent payment order, and whether the originator and the originator's bank's negligence has helped the fraudster to execute the fraudulent EFT. The effects of these types of fraud on the originator and the originator's bank liability will be discussed in Chapters four and five. This section will be restricted to demonstrating types of fraud according to the person who executes the fraudulent EFT.

Maduegbuna has summarized three types of fraud in the context of EFT as follows

> "(T)he possibilities of fraud in the international electronic transfer of funds are many and arise in the same circumstances as in a paper-based payment system. For instance, fraud could arise in an electronic funds transfer system where the originator's employee, perhaps with the connivance of a staff of the originating bank or network provider, activates an unauthorized transfer of funds from the account of the originator. Fraud could also be perpetrated in an electronic funds transfer environment by communications interference, that is, the interception and subsequent change of the transfer instructions to the detriment of the originator. Whatever form fraud takes in an electronic funds transfer system, it is likely to involve an amount far in excess of any fraud

[121] See section 1.2.5 of this chapter for more details about authorised and unauthorised payment order in the context of EFT.
[122] UNCITRAL Model Law in International Credit Transfer 1992 art 5 and Uniform Commercial Law 1989, Article 4A s. 202. See chapter two for more details of unauthorised payment orders.

possible under a paper-based payment mechanism such as the bill of exchange." [123]

The types of fraud in EFT as an electronic payment order are the same in cheques as in paper-based payment orders. Fraud in cheques could be classified according to two types: first, the cheque which bears a forged drawer's signature. This means the payment order is issued and signed by unauthorised person. [124] A second scenario could be where the cheque bears a genuine signature of the drawer, but the cheque details are altered or added to fraudulently by an unauthorised person. [125] In this case, the payment order is issued and signed by an authorised person, but the cheque details are altered by an unauthorised person, such as altering the amount of money or the payee's name. [126]

It is agreed that there are three ways in which a fraudulent payment order may occur in the context of EFT. First, an authenticated payment order is issued and transmitted by an unauthorised person to the bank. [127] For example, when one of the customer's employees issues a payment order to the receiving bank to debit the customer's account and credit his account or a third party's account without the customer's authority. Secondly, an authorised person issues an authenticated payment order, but an unauthorised person alters the payment order details before the payment order is received by the originator's bank. [128] For example, by changing the amount of the payment order or changing the beneficiary's name. Lastly, the originator's bank may

[123]Samuel O. Maduegbuna, "The Effects of Electronic Banking Techniques on the Use of Paper-Based Payment Mechanism in International Trade," J.B.L.1994, Jul, 388-362 at p. 359.
[124] Andrew Laidlaw and Graham Roberts, *Law Relating to Banking Services* 2nded, The Chartered Institute of Bankers, London, 1992 at pp. 124-125 and Graham Roberts, *Law Relating to Financial Services* 5thed, The Chartered Institute of Bakers, Canterbury, 2003 at pp.99-102.
[125] ibid.
[126] ibid.
[127] J. Kevin French, "Article 4A's treatment of Fraudulent Payment Orders-the Customer's Perspective," 1991 42 Ala. L. Rev.773 at p.776 and Maduegbuna, note 123 supra at p.359.
[128] ibid.

receive an amendment issued by an unauthorised person. This amendment is issued to amend the details of an authenticated payment order, which is received by the receiving bank and issued by an authorised person. [129] The unauthorised person, who could execute the fraudulent payment order, may gain access to the customer or the bank's computer terminal or may penetrate the parties' communication. [130]

This person could be one of the customer's employees or one of the bank's employees or a third party. [131]

An employee of the customer might, in the course of his work, be responsible for issuing payment orders, and fraudulently issued or altered payment order in order to be paid in his personal account or a third party account. [132] Moreover, the fraudster could be an employee who unlawfully gains access to the company's computer terminal, and fraudulently issues or alters a payment order to be credited to his account or a third party's account. [133]

The bank's employee may unlawfully obtain the customer's account details and security information, in order to issue unauthorised payment order to credit his account or a third party's account. [134] Alternatively, he may pass the information to a third party, and the third party in turn executes a fraudulent payment order. [135]

Furthermore, a third party may issue a fraudulent payment order or alter the payment order by intercepting the bank customer communications by attacking the security

---

[129] ibid.

[130] Geva 2001, note 43 supra at p.394.

[131] ibid and Jonathan Lass, " Fraud, Error and System Malfunction: A Banker's Viewpoint," Royston Goode (ed), *Electronic Banking: The Legal Implications,* Institute of Bankers, London, 1985, at pp.59-60.

[132] *Agip (Africa) Ltd v Jackson and Others*, [1991] Ch.547.

[133] Arora 1997, note 2 supra at p. 117 and Lass, note 131 supra at p. 59.

[134] Arora, ibid and Lass, ibid.

[135] Attorney General's Reference No.86 of 2003 ( David Parkinson) [2004] 2 Cr. App. R. (S.) 79.

procedures.[136] Alternatively, the third party may obtain the information through the bank's employee or customer's employee.

## 1.2.5.AUTHORISED PAYMENT ORDER AND THE PROBLEM OF IDENTITY AUTHENTICATION IN THE CONTEXT OF EFT

### (a) Significance of Authority

Authority is the result of an agency relationship between the principal and his agent.[137] Thus, in the agency relationship, the principal confers authority to the agent to establish, modify or terminate the legal relationship between the principal and third party. [138] An agent's authority could be classified as actual or apparent. [139] Actual authority occurs where the principal assents expressly or impliedly, such that he confers upon the agent the capacity to act on his behalf in legal relationships. [140] The express actual authority occurs when the principal's express consent is granted by the terms of the contract. With regard to implied (actual) authority, the principal's implied consent could be inferred from the principal's behaviour or words. [141] Lord Denning MR in *Hely-Hutchinson v Brayhead Ltd* [142] stated that

> ".....actual authority may be express or implied. It is express when it is given by words such as when a board of directors pass a resolution which authorises two of their number to sign cheques. It is implied when it is inferred from the conduct of the parties and the circumstances of the case, such as when the board of directors appoint one of their number to be managing director. They thereby impliedly authorise him to do all such things as fall within the usual scope of that office." [143]

---

[136] Arora 1997, note 2 supra at p. 118 and Lass, note 131 supra at p. 59.
[137] F.M.B Reynolds and Michele Graziadei, *Bowstead and Reynolds on Agency,* 18th ed, Sweet & Maxwell, London, 2006 at p.6 and Royston Goode, *Commercial Law*, 3rd ed, Penguin, London, 2004 at p.164.
[138] Goode, ibid .
[139] Reynolds and Graziadei, note 137 supra at p.6.
[140] ibid.
[141] ibid.
[142] *Hely-Hutchinson v Brayhead Ltd* [1968] 1 QB 549 at p. 583.
[143] ibid, at p. 583.

Apparent authority arises as a result of the principal's acts, which leads the third party to believe that a person is an agent of the principal and can act on his behalf, but in fact, either he has not acquired such authority, or he has exceeded that authority. [144] Both the actual and apparent authority of the agent under agency common law is of significance in the context of fraudulent EFT. Firstly, the rules of agency law apply to determine whether the payment order is an authorised payment order or not. Secondly, the application of the rules of agency law in the context of fraudulent EFT raises the problem of identity authentication, and subsequently, the problem of whether the payment order is an authorised payment order or not. [145]

**(b) Authorised EFT and the problem of Identity Authentication**

In EFT, the bank receives the customer's mandate through an electronic access device. For example, an electronic access device could be an open system such as Internet and a closed system such as dedicated network. The customer uses a user name and password to execute the electronic mandate and transmit it to his bank. [146] Thus, if the correct user name and password are used to issue the payment order (mandate), the payment order can be authenticated, and received by the customer's bank through an electronic access device (the Internet or closed system), regardless of whether the person who sends the payment orders is authorised to do so or not. During an electronic payment order transaction, the receiving bank depends on security procedures in order to authenticate the payment order. Due to such authentication, the receiving bank accepts the payment order, as issued by the person

[144] B.S. Markesinis and R.J.C. Munday, *An outline of the Law of Agency,* 3rd ed, Butterworths, London 1992 at p.38.
[145] Hapgood, note 35 supra at p.336.
[146] Hapgood, ibid.

who purported to send it. [147] Thus, in the context of EFT, the bank debits the customer's account depending on an authenticated electronic payment order, regardless of whether the person that sends the payment order is in fact authorised or unauthorised to send such orders. [148] Geva has stated as follows

> "[A] hand written or manual signature is individual to the signer, as such, it identifies the signer. Any signature, other than that of the authorized signer, is by definition unauthorised, and may not serve as a valid authentication on the purported signer's behalf. Conversely, electronic authentication is carried out by means of an access device, which can be entered into a terminal by anyone to whom the device, together with the access to a terminal, becomes available. Electronic Authentication is a means of legitimizing the action of that person, but not identifying the one who actually placed it." [149]

The distinct nature of EFT authentication makes it incomparable with a forged cheque, which could be authenticated by checking the drawer's signature originality. In EFT, meanwhile, banks depend on security procedures to authenticate the payment order. The payment order is authorised if it passes the test of the security procedures.[150] Therefore, Hapgood has rightly argued that "the use of an electronic device access merely authenticates the instruction, it does not identify the person who actually gave it," therefore it is not helpful to decide whether the person who send the payment order an authorised or unauthorised person. Therefore, for the purposes of this thesis an electronic payment order that has been authenticated but has not been authorised by the originator or by a person authorised to do so hereafter in this thesis is referred to it as an authenticated but an unauthorised payment order.

This thesis will demonstrate that under the rules of English agency law, the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT is

---

[147] The Official Comment (1) to the U.C.C section 4A-203 issued by The American Law Institute (ALI) and The National Conference of Commissioners on Uniform State Law(NCCUSL), 1989 ( hereafter the Official Comment of Article 4A)
[148] Hapgood, note 35 supra at p. 336
[149] Geva 2001, note 43 supra at p.395.
[150] Ross Cranston, *Principles Of Banking Law* 2nd ed, Oxford University Press, 2002 at pp. 140-141.

unpredictable and uncertain for the reason that is the rules of agency law are inadequate and inappropriate to deal with the distinctive nature of authentication of electronic payment order. This thesis will argue that in England enacting rules devoted to EFT are needed to determine when an authenticated payment order is an authorised payment order or not. Furthermore, this thesis will argue that the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT should not be left to be regulated by the rules of agency law and contract law. This thesis will argue that under the UNCITRAL Model Law and Article 4A, the originator and the originator's bank's rights, duties and liabilities are more predictable and certain than under English agency law and contract law. The UNCITRAL Model Law and Article 4A contain particular rules to deal with the problem of identity authentication, the problem of authorised and unauthorised payment order and the bank-customer's liability for unauthorised payment order. Accordingly, the rules of the UNCITRAL Model Law and Article 4A, devoted to dealing with the above-mentioned problems, will be examined and assessed in subsequent chapters.

## 1.3 CONCLUSION

The developments of international EFTs networks have increased the number and size of international EFT and have driven the US, EU and UNCITRAL (The United Nations Commissions on International Trade law) to adopt special legal frameworks to regulate such transactions. [151] Heinrich observes that there are three major initiatives to harmonise the rules governing international credit transfers. First, the US Article 4A of the Uniform Commercial Code 1989 (hereafter Article 4A) is adopted by almost all US states. Second, there is the UNCITRAL Model Law in International Credit Transfer 1992. Thirdly, in the EU, the Directive of the European Parliament and of the council on Cross-Border Credit Transfers 1997 (hereafter the EU Directive). [152] The UNCITRAL Model Law was heavily influenced by Article 4A [153] and the EU Directive on Cross-Border Credit Transfers was strongly influenced by the UNCITRAL Model Law. [154] Accordingly, Hapgood has stated that it is not surprising that these frameworks sought to standardise the terminology used for EFT.[155]

The remaining Chapters of this thesis will now examine the existing rules that apply to the originator and the originator's bank's liability for fraudulent international wholesale EFT in England, EU, US and the UNCITRAL Model Law. This thesis will demonstrate that the rules that apply to wholesale EFT in England and the EU do not ensure certainty and predictability of the originator and the originator's bank's rights, duties and liability in the context of fraudulent EFT. Hence, the former rules are not

---

[151] Baker and Brandel, note 72 supra at p.30-11 and Heinrich, note 59 supra at pp. 1 & 11.
[152] Heinrich, note 59 supra at p. 11.
[153] Geva 2001, note 43 supra p.210.
[154] Richard Hooley, "EU Cross-Border Credit Transfers- the New Regime," B.J.I.B. & F.L.1999, 14 (9), 387-395 at p.387.
[155] Hapgood, note 35 supra at p. 291.

adequate and capable of dealing with specific legal issues raise in the context of fraudulent EFT. Namely, the originator and the originator's bank's liability for authenticated but unauthorised payment order. Furthermore, the standard of the security procedures employed by the originator's bank to authenticate the originator's instructions is an issue. Equally important, the scope of the originator and the originator's bank's liability for direct damages and consequential damages arise as a result of fraudulent payment order. Moreover, this thesis will examine the UNCITRAL Model Law and Article 4A treatment of the above-mentioned issues. Furthermore, this thesis will demonstrate that under the UNCITRAL Model Law and Article 4A the originator and the originator's bank's rights, duties and liability in the context of fraudulent EFT are more certain and predictable. The predictability and certainty of the originator and the originator's bank's rights, duties and liability in the context of fraudulent international wholesale EFT, are of significance in executing EFT at high speed, low cost and effectively. This thesis will argue that wholesale EFT law must ensure that the originator and the originator's bank's rights, duties and liability are predictable and certain in the context of fraudulent EFT. Therefore, the EU Directive and the UK regulations should be amended to regulate the originator and the originator's bank rights, duties and liability for fraudulent wholesale EFT.

# CHAPTER TWO

# ANALYSIS OF THE LAW RELATING TO UNAUTHORISED INTERNATIONAL ELECTRONIC FUNDS TRANSFER IN ENGLISH LAW AND EU LAW

## 2.1. INTRODUCTION

The use of communications technology in international electronic funds transfer (EFT) has changed rapidly in recent years, and has greatly improved the operation of international EFT [1] by executing EFT at a higher speed and lower cost. Accordingly, every day millions of cross-border transfers involving huge sums of money are taking place. [2] However, as demonstrated in Chapter one the incorporation of communications technology such as the Internet or dedicated network in international EFT has given rise to new legal problems. The focus of this thesis is on three significant problems -identity authentication, the authenticity of the electronic payment order [3] and the liability of the originator's bank and the originator for unauthorised payment orders as a result of fraud. [4] Chapter two will analyse the law as it applies to identity authentication and an unauthorised electronic payment order in England and the European Union. Meanwhile, Chapter three is an assessment of the rules of the UCITRAL Model Law and Article 4A as they apply to identity

---

[1] "Statistics on Payment and Settlement Systems in Selected Countries," figure for 2002, prepared by the Committee on Payment and Settlement Systems of the Group of Ten Countries, Bank for International Settlements, March, 2004.
http://www.bis.org/publ/cpss60.pdf http://www.bis.org/index.htm (obtained 3/2/2004).

[2] ibid.

[3] Ernest T. Patrikis, Raj K. Bhala and Micheal T. Fois, "An Overview of United States Funds Transfer Law," Robert C. Effros (ed), *Payment Systems of the World*, Oceana Publications, New York, London, 1996 at p. 21 and Donald I. Baker, and Roland E. Brandel, *The Law of Electronic Fund Transfer Systems: Legal and Strategic Planning,* Revised Edition, Warren, Gorham & Lamont, Boston, 1996 at p.30-11.

[4] Baker and Brandel, ibid.

authentication and unauthorised electronic payment orders. Chapters four and five are devoted to examining the liabilities of the originator and the originator's bank for unauthorised electronic payment orders as a result of fraud.

This chapter begins in section 2.2 with an examination of the legal nature of funds transfer under English common law, to determine how the law applies to fraudulent EFT. Section 2.2 will conclude that funds transfer is neither an assignment nor a negotiable instrument. Section 2.3 examines the law as it applies to an unauthorised international EFT in England. Section 2.3 of this chapter will assess the different rules of English common law as they apply to unauthorised EFT. Section 2.3 demonstrates that there is unpredictability and uncertainty in the originator and the originator's bank liabilities for an authenticated but unauthorised payment order. The unpredictability and uncertainty arise as a result of applying the rules of agency law, contract law and drawing analogy with the rules applied to forged cheques. Furthermore, section 2.4 analyses the EU Directive on Cross-Border Credit Transfer. The analysis will examine the scope of the directive and the flaws of the directive in the context of an unauthorised payment order. Section 2.5 examines the UK Regulations on Cross-Border Credit transfer in the context of an unauthorised payment order. Section 2.5 will demonstrate that UK regulations are limited in their scope, as they do not regulate an unauthorised EFT. Therefore, Sections 2.4 and 2.5 of this chapter argue that the EU Directive and the UK regulations need to be amended by adding rules regulating an unauthorised EFT. Section 2.6 focuses on the Jack Committee Report's view of the significance of adopting rules which regulate the security procedures used to authenticate the payment order to protect the bank and its customer from unauthorised EFT. Section 2.7 examines the legal validity of security

procedures as a means of authenticating electronic payment orders in England and EU, as there is no special set of rules devoted to EFT determining the validity of the security procedures used to authenticate electronic payment orders. The examination considers the English common law, the EU Directive on E-signature and its implementation in England. Section 2.7 demonstrates that the former legalisation does not solve the problem of identity authentication on the originator and originator's bank liability for an authenticated but an unauthorised payment order. The purpose of this chapter is to demonstrate that the former issues need to be regulated by particular rules which should be added to the UK Regulations. These rules should take into consideration the security procedures used to authenticate electronic payment orders, as applying the rules of agency or mandate and contract law leads to unpredictable and unfavourable results.

## 2.2 THE LEGAL NATURE OF FUNDS TRANSFER UNDER ENGLISH COMMON LAW

The legal nature of funds transfer is of significance, as it helps to determine the law that governs the banks-customers' rights, duties and liabilities in case of fraudulent EFT. [5] Accordingly, it will be demonstrated in the next two sections that in England, the payment order is a mandate issued by the originator to his bank and it is neither an assignment nor a negotiable instrument. [6] Therefore, contract law and agency law have to be applied to the banks and the customers' liabilities and rights in the context

[5] E. Ellinger, Eva Lomnicka and Richard Hooley, *Ellinger's Modern Banking Law* 4th ed, Oxford University Press, New York, 2005 at pp.542-544.
[6] ibid at p.491, Benjamin Geva, *Bank Collections and Payment Transactions, Comparative Study of Legal Aspects*, Oxford, New York: Oxford University Press, 2001, at p.269 and Richard Hooley and John Taylor, "Payment By Funds Transfer," Michael Q.C. Brindle and Raymond Cox, (eds) 3rd ed, *Law of Bank Payments*, Sweet& Maxwell, London 2004, at p.112.

of fraudulent EFT, rather than the law of negotiable instruments and the principles of assignments. [7]

## 2.2.1. EFT is not an Assignment

There is a consensus in the literature [8] that funds transfer "...involves the movement of a credit balance from one bank account to another, which is brought about by the adjustment of the balances of the payer's bank and payee's accounts, whether at the same or separate banks." [9] Accordingly, in funds transfer, there is no real transfer of coins and banknotes between the originator and the beneficiary. [10] Indeed, what happens is that the originator's bank debits the originator's account and the beneficiary's bank credits the beneficiary's account. [11] Ellinger *et al* rightly opine that the "[T]ransfer of *value*, rather than the transfer of funds, is probably more accurate description of the giro process [funds transfer process]. [12] " [13]

According to case law [14] the legal nature of funds transfer is an authority conferred by the customer on the bank. In *Royal Products Ltd v. Midland Bank Ltd* [15] Webster J stated:

> "[W]hat, then are the legal implications of those instructions? [funds transfer][16] How are they to be regarded, as a matter of law? In my judgement

[7] Ellinger, Lomnicka and Hooley , ibid at p.513, Geva 2001, ibid and Hooley and Taylor, ibid.
[8] Hooley and Taylor, ibid at 49, Ellinger, Lomnicka and Hooley, ibid, and Mark Hapgood, QC, Paget's Law of Banking 12th ed, Butterworths, London 2002 at p. 291.
[9] Hooley and Taylor, ibid.
[10] Hooley and Taylor, ibid and Ellinger, Lomnicka and Hooley, ibid.
[11] Hooley and Taylor, ibid. and Ellinger, Lomnicka and Hooley, ibid.
[12] Words in square brackets added .
[13] Ellinger, Lomnicka and Hooley, ibid 514.
[14] *Barclays Bank Plc v Quincecare Ltd*, [1992] 4 All ER 363, *Comptroller of Stamps v Howard Smith*, (1936) 54 CLR 614 and *Libyan Arab Foreign Bank v Banker's Trust Co* [1988] 1 Lloyd's L.R. 259 (Q.B).
[15] *Royal Products Ltd v Midland Bank Ltd* [1981] 2 Lloyd's Rep.
[16] Words in square brackets added.

> they are to be regarded simply as an authority and instruction, from the customer to its bank, to transfer an amount standing to the credit of that customer with that bank to the credit of its account with another bank, that the other bank being impliedly authorised by the customer to accept that credit by the virtue of the fact that the customer has required of that other bank, by virtue of the same fact. It is, in other words, a banking operation, of a kind which is often carried out internally, that is to say, within the same bank or between two branches of the same bank and which, at least from the point of view of the customer, is different in nature or quality when, as in the present case, it is carried out between different banks." [17]

The above judgement ascertains that the funds transfer is carried out by the originator's bank between different accounts in different banks according to the authority conferred by the customer to its bank. [18] Moreover, in *Libyan Arab Foreign Bank v Bankers Trust Co.* [19] Staughton J. has affirmed that funds transfer is not an assignment, and his view been confirmed by the House of Lords in *R v Preddy.*[20] Staughton J stated

> ""Transfer " may be a somewhat misleading word, since the original obligation is not assigned (notwithstanding dicta in one American case which speak of assignment); a new obligation by a new debtor is created." [21]

Hapgood has meanwhile explained that the originator does not assign his rights towards the originator's bank to the beneficiary or the beneficiary's bank. [22] The funds transfer instruction could be revoked until the time the payment orders become irrevocable, for example, before it reaches the recipient bank, whilst the assignment order would be irrevocable once it is complete. [23] Ellineger *et al* have emphasized

---

[17] *Royal Products Ltd v Midland Bank Ltd*, note 15 supra at p. 197
[18] Ellinger, Lomnicka and Hooley, note 5 supra at p. 547.
[19] *Libyan Arab Foreign Bank v Banker's Trust Co*, note 14 supra, applied by the Court of Appeal in *Customs and Excise Commissioners v FDR Ltd*, 2000 WL 877741.
[20] *R. v. Preddy* [1996] 2 Cr. App. R. 524 HL, applied by the Court of Appeal in *R. v Clark (Brian James)*, [2002] 1 Cr. App. R. 14
[21] *R. v. Preddy* ,ibid at p.273.
[22] Hapgood, note 8 supra at p. 333
[23] Hooley and Taylor, note 6 supra at p. 102.

that the funds transfer operation is not a statutory assignment, for two reasons; first, in funds transfer the customer usually instructs the bank to transfer part of the debit owed by the bank to its customer. Thus, the order to transfer part of the debit is not approved by section 136 of the Law of Property Act 1925. [24] Second, the customer may not have any outstanding credit at the time of issuing the funds transfer, as the customer believes that the amount required to complete the transaction will be available at the time the transfer is to be affected. Thus, the assignment of future debit is not recognised by section 136 of the Law of Property Act 1925. [25]

Furthermore, all types of funds transfer, for instance, bank giro credit, CHAPS and facsimile are services offered by the bank to its customer. Thus, sometimes the customer does not ask for outstanding credit transfer, but the customer may ask for an overdraft extension, accordingly the bank is not always the customer's debtor. [26] Hence, the international EFT is a credit transfer and operates in the same way that the domestic EFT operates. [27] According to the common law the international wholesale EFT is not an assignment and the Law of Property Act 1925 does not apply to such transactions.

---

[24] Ellinger, Lomnicka and Hooley, note 5 supra at pp.546-547.
[25] ibid.
[26] ibid.
[27] ibid, at p.520 and Hooley and Taylor, note 6 supra at p. 58.

## 2.2.2 EFT is not a Negotiable Instrument

Under Section 3 of the Bill of Exchange Act 1882, for a funds transfer instrument to be a negotiable instrument, it should contain specific requirements. First, it must be an "unconditional order" in writing; second, it must be addressed by one person to another, and lastly, instructing the addressee to pay on demand or at a fix or determinable future time a specific amount of money to the payee. According to the former definition, there is a consensus that paper-based funds transfer and EFT is a not negotiable instrument. [28] In regards to EFT, it lies beyond the scope of the definition of a negotiable instrument, as it is not a written payment order and is issued by using electronic means such as SWIFT and CHAPS. [29] Furthermore, the negotiable instrument should be payable for a specified person or bearer, whilst a paper-based or electronic funds transfer is payable to a specific payee in his account. Since the negotiable instrument is payable on sight or on payee demand, the funds transfer falls outside the definition. As a funds transfer is not payable on demand or within a determinable time, it is payable once the originator has issued the payment order. [30] Ellinger *et al* have emphasized that

> "..most important ground for treating a bank giro credit [credit transfer] as falling outside the definition of a negotiable instrument is that the giro form does not include any words that can be construed as a formal instruction given by the originator ( payer) to the originator's bank. Accordingly the form is not an order. This point is true in respect of all giros used in the United Kingdom. It follows that these forms do not constitute negotiable instruments. The conclusion that giro forms do not constitute negotiable instruments is of considerable practical importance in instances of deceit. Where a giro form is fraudulently issued or altered, the rights of the parties depend on principles of the law of contract and of agency alone; the law of negotiable instruments is inapplicable. " [31]

---

[28] Ellinger, Lomnicka and Hooley ,ibid at p. 544 and Hooley and Taylor, ibid at p. 116.
[29] Ellinger, Lomnicka and Hooley ,ibid and Hooley and Taylor, ibid pp.116-117.
[30] Ellinger, Lomnicka and Hooley, ibid at p.545 and Hooley and Taylor ibid at 117.
[31] Ellinger, Lomnicka and Hooley, ibid.

Hapgood has confirmed that no type of credit transfer by the originator to the originator's bank to deposit a specific amount of money to the beneficiary's account in his bank is a negotiable instrument, despite the means that have been used to issue the payment order, for example, letter, facsimile, telex and CHAPS. [32]

In the *Tenax Steamship Co Ltd v The Brimnes* [33] the court decided, according to the law mercantile and the Bill of Exchange Act 1882, that a fund transfer issued by telex is not a negotiable instrument, and is not equal to a cheque. Cairns LJ stated as follows:

> "[T]he property in money passes on delivery; so does the property in a cheque. Partly by operation of the law merchant and the Bills of Exchange Act 1882, partly by the customs of business, cheques have become regarded as the equivalent of money (subject always to being afterwards defeated by dishonour). I do not think that the telex message in this case can be regarded in the same way. It was not a negotiable instrument. It could have been revoked by [the payer's bank] at any time before being acted upon by the [payee's bank], and if it had been so revoked, no action could have been brought on it as it could no a stopped cheque." [34]

Under common law, the negotiable instrument must be capable of being transferred from one person to another by endorsement and delivery like cheques. Moreover, negotiable instruments give the *bona fide* holder of the cheque a title for its value, which is not affected by the defects of title of previous parties. [35] Hence, paper-based or electronic funds transfer payment orders are not capable of being transferred to another person, and do not give the bona fide holder a title of value such transaction falls out the ambit of negotiable instruments.

---

[32] Hapgood, note 8 supra at p. 333.
[33] *Tenax Steamship Co Ltd v The Brimnes*,[1975] 1 Q.B. 929. approved by the House of Lords in *Mardorf Peach & Co Ltd v Attica Sea Carriers Corp of Liberia*, [1977] 2 W.L.R. 286 and applied by the House of Lords in *Awilco of Oslo A/S v Fulvia SpA di Navigazione of Cagliari (The Chikuma)*, [1981] 1 W.L.R. 314.
[34] *Tenax Steamship Co Ltd v The Brimnes,* ibid at p. 969.
[35] *Crouch v Credit Foncier of England* (1873) L.R. 8 Q.B.374 at 381-382, Hapgood, note 8 supra at p.334 and Hooley and Taylor, note 6 supra at p.116.

In conclusion, under common law, the international wholesale EFT is not a negotiable instrument, and the Bill of Exchange Act 1882 is not applied to the originator and the originator's bank's duties, rights and liabilities for fraudulent EFT. As Ellinger *et al* stated in the case of fraudulent EFT the law of contract and agency are applied to determine the parties' duties, rights and liabilities. [36] Further, Geva has confirmed that the originator and the originator's bank's rights, duties and liabilities are regulated by drawing an analogy with the rules apply to forged cheques. [37] The next section examines the law of contract, the law of agency and the rules that apply to forged cheques as they apply to an unauthorised EFT. It demonstrates that the application of these laws to authenticated but unauthorised payment order is inadequate and inappropriate in determining the originator and the originator's rights, duties and liabilities. Subsequently, applying the law of contract and agency to an authenticated but an unauthorised payment order leads to uncertainty and unpredictability in the originator and the originator's bank's rights, duties and liabilities.

[36] Ellinger, Lomnicka and Hooley, note 5 supra at p. 545.
[37] Geva 2001, supra not 6 at p. 393.

## 2.3. A CRITIQUE OF THE RULES APPLYING TO UNAUTHORISED EFT IN ENGLISH LAW

### 2.3.1 The Law of Agency and The Problem of Identity Authentication

The agency relationship between the bank and its customer exists in respect of payments and collections by the bank on behalf of the customer. [38] The principal and agent relationship arises when the originator's bank accepts the originator's mandate and transfers funds to a third party in different country through electronic means. Indeed, the bank executes paying or collecting payment orders according to the customer mandate. [39] In the *Royal Products Ltd v Midland Bank Ltd* [40] case, which was brought before the Queen Bench Division, the plaintiffs had a current account with the defendants, Midland Bank, the National Bank of Malta and the Bank of Industry, Commerce and Agriculture Ltd in Malta (BICAL). The plaintiffs instructed the Midland Bank to transfer £13,000 by cable to BICAL. The Midland bank cabled their correspondent in Malta the National bank instructing them to transfer money to BICAL. The national bank credited the money in a suspense account in the name of BICAL and informed them. The National bank knew that BICAL were facing financial problems, but the Central Bank in Malta confirmed that BICAL would be open the next day. The next day, BICAL ceased business and the plaintiffs sued the National Bank and the Midland bank. The defendant claimed *inter alia* that they were entitled to the return of their money on the basis that the national bank were their agents and were in breach of their duty of care in making the transfer when they knew about BICAL difficulties. Moreover, Midland were liable for National's breach, and even if National were not their agent, National owed them a duty of care of which

---

[38] Arora, *Electronic Banking and the Law* 3rd ed, IBC Business Publishing, UK, 1997 at p. 77.
[39] Geva 200, note 6 supra at p.89.
[40] *Royal Products Ltd v Midland bank Ltd,* note 15 supra.

they were in breach. In *Royal Products Ltd v Midland bank Ltd*, [41] Webster J held that the relationships between the paying bank and its customer or the intermediary in the context of a funds transfer transactions are governed by agency law. [42] Webster J has emphasized that in funds transfer the paying bank owed the customer a duty of reasonable care and skill and the paying bank will be liable for the breach of that duty by its agent or servant. [43] Moreover, there is no direct relationship between the intermediary bank and the customer; therefore the intermediary bank does not owe the customer any duty of care.[44] Webster J has stated as follows:

> "... [I] hold that it was, it follows that in carrying out its part of the transaction Midland [the originator's bank] [45] owed Royal Products [the originator] [46] a duty to use reasonable care and skill...and that they would be vicariously liable for the breach of that duty by any servant or agent to whom they delegated the carrying out of the instructions. Midland, therefore, would be liable to Royal Products for National's negligence [intermediary bank], [47] if any, in that respect. But in my judgment National owed no duty of any kind direct to Royal Products. ...In my judgment, therefore, National are not to be regarded as having been agents of Royal Products and did not, therefore, owe them any of the duties, including a fiduciary duty, owed by an agent to his principal." [48]

Accordingly, the originator and originator's bank's rights, duties and liability in the context of fraudulent EFT are governed and regulated by agency law. [49] Webster J has emphasized that in funds transfer, the paying bank owed the customer a duty of reasonable care and skill and the paying bank will be liable for the breach of that duty by its agent or servant. [50] Moreover, there is no direct relationship between the

---

[41] ibid
[42] ibid 198.
[43] ibid.
[44] ibid.
[45] Words in square brackets added.
[46] Words in square brackets added.
[47] Words in square brackets added.
[48] *Royal Products Ltd v Midland Bank Ltd*, note 15supra at p. 198.
[49] Geva 2001, note 6 supra at p.104 and Razeen Sappideen, "Cross-Border Electronic Funds Transfers Through Large Value Transfers Systems and the Persistence of Risk," 2003, J.B.L., pp.584-602 at p.584
[50] *Royal Products Ltd v Midland Bank Ltd*, note 15 supra at p. 198.

intermediary bank and the customer; therefore the intermediary bank does not owe the customer any duty of care.[51]

In England it is submitted that EFT is a mandate from the originator to the originator's bank, authorising the bank to conduct a funds transfer. [52] Thereby, the general principle rules of agency law or mandate law apply to EFT. According to the Court of Appeal's decision in *Fielding v Royal Bank of Scotland Plc* [53] the bank's authority arose as a result of a customer's mandate to his bank. [54] Moreover, Parker L.J explained that, as long the bank acts within the remit of the mandate, it is entitled to debit the customer's account, because the bank has the authority to pay such a cheque. [55] Geva has stated that unauthorised transfers in the context of EFT transactions:

> "[M]ust emanate [the payment order] [56] from someone who either assumed control of the accesses device unlawfully, or bypassed the access device altogether. Such a person may be a member of the customer's household, the customer's employee or associate, or total stranger." [57]

Conversely, an authorised payment order is a mandate initiated by the customer or by a person authorised by the customer to issue a payment order. Consequently, to execute an authorised funds transfer on behalf the customer, the bank should have the customer's consent, taking into consideration that the authorisation and its limitations may be provided by the current account agreement or a specific agreement for EFT. These agreements set out the circumstances and the conditions for an authorised payment order. [58] Thus, an authorised payment order is required to be executed upon the customer's mandate or the person the customer authorised to do so and within the

---

[51] ibid.
52 ibid and Benjamin Geva 2001, note 6 supra at p.212,
[53] *Fielding v Royal Bank of Scotland Plc* [2004] WL 62144 .
[54] ibid, at para.56.
[55] ibid.
[56] Words in square brackets added.
[57] Geva 2001, note 6 supra at p.394.
[58] Benjamin Geva, *The Law of Electronic Funds Transfers; Global and Domestic Wire Transfers*, ACH payments, Consumer Transactions, Mathew Bender, New York, 1994 at p.2-66.

customer's instructions. The bank that executes a payment order outside the customer's mandate is not entitled to debit the customer's account, depending on that payment order, as it is an unauthorised payment order. [59] Arora has confirmed that the bank is under a duty to adhere to the customer mandate and the bank cannot debit the customer's account beyond the limit of the customer mandate.[60]

However, the present author's view is that applying the rules of mandate does not give the bank the required protection. Thus, the bank will be reluctant to execute the payment order entirely or may choose not to execute it at high speed or at a low cost. The reason for such reluctance is that the bank, through the electronic access whether to an open or closed network, is unable to determine whether the person who sends the payment order is authorised by the customer himself or his actual or apparent authority. As indicated in Chapter one, [61] the bank which receives payment orders through electronic methods is unable to determine the identity of the person who sends such an order. The issue of identity authentication is important in determining whether the person who sends the payment order is authorised to do so. This is because the bank is not allowed to debit the customer's account depending on a forged or unauthorised mandate. [62] In *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd.* [63](Privy Council) Lord Scarman J has stated:

> " The business of banking is the business not of the customer but of the bank. They offer a service, which is to honour their customer's cheques when drawn upon an account in credit or within an agreed overdraft limit. If they pay out

---

[59] Ross Cranston, *Principles Of Banking Law* 2nded, Oxford University Press, 2002 at p. 140-141 and Ross Cranston, "Law of International Funds Transfer in England," Walther, Hadding and Uwe H. Schneider, (eds), Legal Issues in International Credit Transfers, Duncker & Humblot, Berlin, 1993 at p.224.

[60] Arora 1997, note 38 supra at p.84.

[61] Chapter one section 1.2.5(b).

[62] Hapgood, note 8 supra at p. 336.

[63] *Tai Hing Cotton Mill Ltd. V Liu Chong Hing Bank Ltd.and others* [1985] 2 Lioyd's Rep.313 PC, followed by *Patel v Standard Chartered Bank*, [2001] Lloyd's Rep. Bank. 229.

> upon cheques which are not his, they are acting outside their mandate and can not plead his authority in justification of their debit to his account. This is a risk in the service which it is their business to offer." [64]

In the context of EFT, it is not possible for the bank to determine the identity of the person who sends the payment order, making it difficult to decide whether to accept the payment order or refuse it. [65] In other words, the bank cannot determine whether the payment order has been authorised by the originator or not. Therefore, there is a significant relationship between identity authentication and the rules of mandate, as they combine to determine whether the payment order is authorised or not and to decide whether the bank is entitled to debit the originator's account by the sum detailed on the payment order. Under English case law such as *Greenwood v Martins Bank Ltd,* [66] *London Joint Stock Bank, Limited v Macmillan and Arthur* [67] *and Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd* [68] the bank is not entitled to debit the customer's account when the customer's signature on a cheque or a mandate has been forged. The present author's view is that applying rules of mandate law to EFT leads to the conclusion that authenticated payment orders are authorised only when initiated by an authorised person. Subsequently, an authenticated payment order issued by an unauthorised person is an unauthorised payment order, and the bank cannot debit the customer's account. Accordingly, under agency law the originator's bank's liability for authenticated but unauthorised payment order is unpredictable and certain.

---

[64] *Tai Hing Cotton Mill Ltd,* ibid at p. 321.
[65] Hapgood, note 8 supra at p. 336.
[66] *Greenwood v Martins Bank Ltd* [1933] AC 51, approved by *Tai Hing Mill Ltd. V Liu Chong Hing Bank Ltd.and others* [1985] 2 Lioyd's Rep.313 PC and followed by *Patel v Standard Chartered Bank,* [2001] Lloyd's Rep. Bank. 229.
[67] *London Joint Stock Bank, Limited v Macmillan and Arthur,* [1918] A.C.777, approved by *Tai Hing Mill Ltd. V Liu Chong Hing Bank Ltd.and others* [1985] 2 Lioyd's Rep.313 PC and applied by *National Bank of New Zealand v Walpole and Patterson,* [1975] 2 N.Z.L.R. 7.
[68] *Tai Hing Mill Ltd,* note 63 supra.

Finally, the position of unauthorised EFT has been analogised with a forged or unauthorised cheque. [69] Pennington has explained that if the bank acts on an unauthorised payment order, it would be the same as a bank paying a forged and unauthorised cheque. [70] The legal consequence for a bank which acts on a forged and unauthorised cheque exists in section 24 of the Bills of Exchange Act 1882, which states:

> " [S]ubject to the provisions of this Act, where a signature on a bill is forged or placed thereon without the authority of the person whose signature it purports to be, the forged or unauthorised signature is wholly inoperative, and no right to retain the bill or to give a discharge therefore or to enforce payment thereof against any party thereto can be acquired through or under that signature, unless the party against whom it is sought to retain or enforce payment of the bill is precluded from setting up the forgery or want of authority.
> Provided that nothing in this section shall effect the ratification of an unauthorised signature not amounting to a forgery."

Section 24 states that a forged or unauthorised signature of a bill is wholly inoperative and does not confer any rights on the holder of the bill. Moreover, the bank that pays a forged cheque acts outside the customer mandate, and cannot debit the customer's account. In view of this, Arora has stated that in conventional paper-based transactions, the bank cannot debit the customer's account on the strength of a forged cheque, as it has no mandate to allow this. Therefore, the bank is obliged to credit the customer's account with the amount it has debited. [71] Accordingly, in wholesale EFT, if a payment order is given by a person who acts without the customer's authority or beyond the authority given by the customer, the bank cannot debit the customer's account, as it is an unauthorised payment order. [72]

However, Smart has aptly argued as follows:

---

[69] Robert Pennington, "Fraud, Error and System Malfunction," Royston Goode, *Electronic Banking: The Legal Implications*, Institute of Bankers, London 1985 at p.70 and Arora 1997, note 38 supra at p.120.
[70] Pennington, ibid.
[71] Arora 1997, note 38 supra at p.120.
[72] ibid .

> " [T]he optimist may suggest that there is nothing fundamentally new in electronic funds transfer; it is merely a variety of novel methods of transferring funds from D to C, and in banking legal problems will be solved by analogy with existing law. The relationship of banker and customer is fairly well settled, and all that will be needed is the fitting of changed methods into an established framework. But optimism, based on a partial truth, oversimplifies the matter. Certainly the cheque, which commits the paying banker only when he decides to pay it (and which gives the unpaid payee a right of action against the drawer), is an uncertain basis for analogy." [73]

The present author's view is that using electronic means to verify the payment order gives rise to the problem of identity authentication and, therefore, makes unauthorised EFT incomparable to forged cheques. Geva argues that the bank's duty to detect and prevent unauthorised payments differs according to the methods of authentication used to verify forged cheques and unauthorised EFT. [74] Geva has further illustrated that in the case of forged cheques, the bank examines and investigates the written signature on every cheque to determine whether the cheque is authenticated and then authorised, [75] while in EFT, the bank implements security procedures verify the electronic payment order to determines whether it is authorised or not. [76] Hapgood argues that the hand-writing signature identifies the signer of the cheque, as it is individual, whereas security procedures authenticate the transaction itself and they do not identify the person who sends the payment order. Accordingly, determining the originator and the originator's bank's liability for authenticated but unauthorised payment order in the context of EFT, by drawing analogy with the rules which apply to the loss allocation in the case of forged cheques, leads to unpredictability and uncertainty in the parties' liabilities.

---

[73] Eynon Smart, "Electronic Banking: An Overview of the Legal Implications", Royston Goode, *Electronic Banking: The Legal Implications,* Institute of Bankers, London 1985 at p.1.
[74] Geva 2001, note 6 supra at p. 395.
[75] ibid.
[76] ibid.

### 2.3.2 The Law of Contract and Unfair Terms Contract Imposed on the Originator

The bank-customer relationship starts from the moment the customer has decided to open a bank account. [77] There is a consensus [78] that the basic relationship between the bank and its customer is regulated by the common law of contract. [79] Therefore, the bank-customer relationship as a rule is governed by the contract (account agreement) entered into between the bank and the customer. [80] Moreover, the account contract contains implied terms, which are unwritten and stipulate the legal obligations imposed on the parties. [81] Currently, banks provide their customer with a separate express written agreement for particular services. [82] This include, credit and debit cards and accesses to the bank services via telephone or Internet. [83] EFT is one of the bank services which the customer accesses thorough electronic means; thereby EFT might be regulated by express separate agreement. The current account agreements and the separate written agreement for particular services are "standard form contracts" prepared by banks. When customers open a bank account, they usually agree to be bound by the standard terms.[84]

Since in England, the common law of contract governs the bank-customer relationship in the context of fraudulent EFT, banks in their contracts try to limit and avoid liability for authenticated but unauthorised payment order. By stipulating in express

---

[77] Geva 2001, note 6 supra at p.25 and Anu Arora, *Cases and Materials in Banking Law*, London: Pitman c1993 at p. 77.
[78] Milnes Holden, *The Law and Practice of Banking*, Vol.1, Banker and Customer 5thed, Pitman, London 1991 at p.50. J. Wadsley and A.G. Penn, *The Law Relating to Domestic Banking* 2nded, Sweet& Maxwell, London 2000 at p.103 and Arora 1993, ibid.
[79] Holden, ibid, Wadsley and Penn, ibid and Arora 1993, ibid.
[80] Geva 2001, note 6 supra at p.25 and Arora 1993, ibid at p. 77.
[81] Holden, note 78 supra at p.50, Wadsley and Penn, note 78 supra at p. 104 and Arora 1993, ibid.
[82] Wadsley and Penn, ibid and Ellinger, Lomnicka and Hooley, note 5 supra at p.125.
[83] Ellinger, Lomnicka and Hooley, ibid.
[84] Geva 2001, note 6 supra at p.30.

written terms that they are not liable to pay back the money that has been debited from the

customer's account according to authenticated but unauthorised payment order. [85] Unlike the consumer customer exclusive and limiting conditions are binding against the business customer, as there is no legislation devoted to protect business customer from such conditions. [86] The present author's view is that business customers need to be protected from exclusive and limiting conditions on the basis that not all business customers can negotiate or reject the standard contract terms. It is more to likely that small and medium business customers cannot negotiate or reject exclusive and limiting conditions because of the disparity of bargaining power. Geva has confirmed that standard form contracts could be used towards small customers, particular consumer and large corporate customers. [87]

In England, the consumer customer is not bound by unfair contract terms incorporated in the "standard contract terms," for the reason that the terms of the consumer customer [88] account agreement need to satisfy the Unfair Terms in Consumer Contracts Regulations 1999 ( hereafter UTCCR) and the Unfair Contract Terms Act 1977 (hereafter UCTA). [89] In contrast, the business customer is probably bound by terms which limited or exclude the bank's liability for authenticated but unauthorised payment order executes by third party or as a result of the intermediary bank's

---

[85] Ahmed Azzouni, "Internet banking and the Law: a critical examination of the Legal controls over Internet banking in the UK and their ability to frame, Regulate and secure banking on the net," J.I.B.L.R. 2003, 18(9), 351-362 at p.361, Maria C Malaguti, " Legal Issues in Connection with Electronic Transfers of Funds," L.C. & A.I. 1992, 1(3), 275, at p. 284.
HSBC, Business Internet Banking (BIB) Terms and Conditions.
http://www.hsbc.co.uk/1/2/business/online-services/terms-conditions (Obtained on 15/05/06).

[86] Ellinger, Lomnicka and Hooley, note 5 supra at p.126.

[87] Geva 2001, note 6 supra at p.30.

[88] The Consumer customer in the Unfair Terms in Consumer Contracts Regulations 1999, regulation 3 (1) is " means any natural person who, in contracts covered by these regulations, is acting for purposes which are outside his trade, business or profession."

[89] Ellinger, Lomnicka and Hooley, note 5 supra at, p.552 and Hapgood, note 8 supra at p.338

negligence. As such, clauses might be found reasonable against business customers under the UCTA, on the basis that the originator's bank does not acquire control over the intermediary bank. [90] Ellineger *et al* have stated that "...the customer may still need to rely to a variety of general common law and statutory techniques to police the banking contract. In this respect the consumer customer is better served than the business customer." [91] Moreover, Geva has confirmed:

> " [Y]et jurisprudence on this point [exemption clauses] [92] has not been fully settled, and so far, there is no unequivocal common law authority precluding exemption clauses aimed at either exonerating a bank from its own negligence or passing on liability to a non-negligent customer." [93]

On February 2005 a joint report on Unfair Contract Terms and a Draft Unfair Contract Terms Bill and Explanatory Note were published by the Law Commission and the Scottish Law Commission. [94] The report focused on two main statutes dealing with unfair contract terms in UK, firstly the UCTA, and secondly, the UTCCR. Both of them currently regulate unfair contract terms. [95] The report recommended incorporating the two statutes into a " single unified legislative regime" which must provide the customer with the same protection presently granted by both legislation. [96] The report recommended that protection should be given to small businesses just like as the protection given to consumers under UTCCR against unfair contract terms. [97] However, the report and the draft bill have been exempted from protection. Firstly, for the business customer who has more than nine staff, and secondly, the small business

---

[90] Ellinger, Lomnicka and Hooley, ibid and Hapgood, ibid.
[91] Ellinger, Lomnicka and Hooley, ibid at p.126.
[92] Words in square brackets added.
[93] Geva 2001, note 6 supra at p. 99-100.
[94] The Law Commission and the Scottish Law Commission Report on Unfair Terms in Contracts, 31 December 2004.
http://www.lawcom.gov.uk/docs/lc292.pdf (obtained 16/02/2007)
http://www.lawcom.gov.uk/
[95] ibid, p.1.
[96] ibid, p.8.
[97] ibid, p.17.

associated with larger business. Thirdly, contracts involving transaction value in excess of £500, 000 are also exempted and lastly, financial services contracts. [98] Accordingly, the draft bill does not provide the originator with protection against exclusive and limiting conditions stipulated in the contract which govern the originator and the originator's bank relationship in the context of fraudulent EFT. The Draft Unfair Contract Terms Bill was laid before the Parliament of United Kingdom and the Scottish parliament on 25 February 2005 when the report of the law commission report was published, and did not come into force during the period of writing this thesis.

Moreover, Thunis has pointed out, however, that there are separate contracts to regulate different bank services. These contracts contain in common the terms which govern the access of services and the customer's obligation to protect the means of access. Moreover, the contracts contain in common the conditions which regulate the bank and the customer's liability in cases of loss or theft, and permissible evidences and factors of proof which are accepted as proof that the operation is executed. [99]

In the context of EFT contracts Thunis has argued that the bank, as provider of financial services, is in an economically dominant position, as it stipulates conditions and terms that seek to limit its liability [100] against any fraud or unauthorised mandates executed by a third party. [101] Moreover, banks may stipulate clauses which broaden the concept of *force majeure*. These clauses aim to avoid any liability if the bank fails to fulfil its obligations against the customer, due to many reasons such as, the network

---

[98] ibid, p.18 and Draft Unfair Contract Terms Bill, cls 27,28 and 29.
[99] Xavier Thunis, Recent Trends Affecting The Banks' Liability During Electronic Funds Transfer, J.I.B.L. 1991,p. 297-309 at p.299-300
[100] ibid.
[101] Azzouni, note 85 supra at p. 360-361 and Thunis, ibid at p.300.

malfunctions or errors and fraud. [102] Furthermore, Ellinger *et al* have affirmed that the originator's bank which executes EFT by employing an intermediary bank, incorporates terms in the contract with its customer that exclude the bank from liability for an intermediary bank's negligence. [103] The present author's view is that all such clauses are unfair, as they deprive the customer of the right to sue the bank for damages or money refund as a result of an authenticated but unauthorised payment order. Moreover, the originator is not entitled to sue the intermediary bank for refund or damages as there is no agency or contractual relationship between them. Consequently, the originator bears the liability for authenticated but unauthorised payment order executed by a third party and without the originator's negligence. Such clauses are unfair because the security procedures used in funds transfers and intercepted by a third party are implemented and chosen by the bank. Thunis has stated as follows:

> "[I]f the fraud has been facilitated by an adequate security system implemented by the bank, it appears that the bank's liability is brought into play. Although it is true that the customer (a company and, therefore, a professional) chooses his means of payment, the banker (as professional credit organisation) should be held primarily responsible for the data processing system he offers for organising and rationalising his bank services." [104]

In conclusion, in England there is no "comprehensive statutory regime" for EFT governs the bank and customer's liabilities for authenticated payment orders, whether such payment orders are in fact authorised or unauthorised. Therefore, in order to avoid the bank's liability for authenticated but unauthorised transactions, banks incorporate in their contracts with customers express terms that such transactions are

---

[102] Thunis, note 99 supra at p.299-300.
[103] Ellinger, Lomnicka and Hooley, note 5 supra at p.551.
[104] Thunis, note 99 supra at p. 300.

authorised. [105] Thus, banks are entitled to debit the customer account with the amount of money detailed on the payment order and there is no limit for customer liability. [106] Moreover, banks exclude themselves and limit their liability for unauthorised payment orders and allocate the risk to the customer. [107] By contrast, in the absence of a contract between the bank and its customer, agency law must be applied. According to agency law, the bank will be liable for authenticated but unauthorised payment orders, and such rules do not give the bank the protection they seek. The present author's view is that whether there is an agreement or not, both scenarios lead to extremes in liability for an unauthorised payment order. Neither party apportions blame for the unauthorised payment order between the originator and the originator's bank, but one of them bears the entire liability. The present author argues that the originator and the originator's bank's liability for authenticated but unauthorised payment order should be regulated by rules devoted to EFT. Such rules determine whether the originator's bank is entitled to debit the originator's account according to authenticated but unauthorised payment order. Moreover, rules are needed to protect the originator from unfair terms contract which exclude or limit the originator's bank's liability for authenticated but unauthorised payment order executed by a third party without the originator's negligence. In other words, there should be rules that allocate the liability for authenticated but unauthorised payment order between the originator and the originator's bank. Such rules must make the originator and the originator's bank's rights, duties and liabilities more predictable and certain than under English law.

[105] Hapgood, note 8 supra at p.336.
[106] Ahmed Azzouni, note 85 supra at p360.
[107] ibid.

In 1999 the Cross-Border Credit Transfers Regulations 1999 came into force as an implementation to the EC Directive 97/5 on Cross-border Credit Transfers in UK. [108] The EC Directive on Cross-Border Credit Transfers was strongly influenced by the UNCITRAL Model Law. [109] Thus, it is not surprising that these frameworks sought to standardise the terminology used for EFT. [110] Nevertheless, the EU Directive and the UK Regulations do not regulate the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT, which the UNCITRAL Model law deals with. The following two sections are an assessment of the rules of the EU Directive and the UK Regulations in the context of an unauthorised EFT. The following examination will start by looking at the EU directive before the UK Regulation. The present author's view is that starting with the EU directive helps to elaborate the effects of the EU directive on the UK Regulations. The following sections will demonstrate that the rules of the EU Directive and the UK Regulations do not regulate the originator and the originator's bank's liabilities for authenticated but unauthorised EFT. In addition, neither both legislation devote any rules to determining the standards of security procedures which should be applied by the originator's bank to authenticate the payment orders. Nor do they devote any rules to determine the standards of security procedures which should be employed by the originator's bank to authenticate the originator's payment order.

[108] Cross-Border Credit Transfer Regulations 1999, 1999 No 1876 and Ellinger, Lomnicka and Hooley, note 5 supra at p.554 and Hapgood, supra note 8 at p. 330.
[109] Richard Hooley, "EU Cross-Border Credit Transfers- the New Regime", B.J.I.B. & F.L.1999, 14(9), 387-395 at p.387.
[110] Hapgood, note 8 supra at p. 291.

## 2.4. THE EU DIRECTIVE AND AN UNAUTHORISED EFT

### 2.4.1 The Objectives of the EU Directive

Indeed, the preamble of the EU Directive on Cross-Border Credit Transfers 1997 illustrates expansively the factors that prompted the European Parliament and the European Council to adopt this directive. [111] Since then, the EU has sought to achieve progress in the internal market by way of full economic and monetary union, therefore it calls for an efficient and secure payment system, which facilitates cross-border payments. [112]

Furthermore, an issue of equal importance is that the EU seeks to enhance customer protection and improve the level of cross-border credit transfer services; [113] it also seeks greater competition and cost reduction. [114] Thus, the EU Parliament has decided that such goals can be achieved by adopting the Cross-Border Credit Transfer Directive, which regulates the parties' rights, obligations and liabilities for cross-border EFT. Thus, the consumer and small and medium sized enterprises (SMEs) become more confident that they can transfer money reliably, inexpensively and swiftly. [115]

In addition, the EU Directive sets out the duration for the execution of a cross-border credit transfer and enforces an obligation for the financial institution to inform

---

[111] Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, OJ L 043, 14/02/1997 P.25 – 30.
[112] ibid the EU Directive, preamble (1) and Reinhard Steennot, "The Single Payment Area," J.I.B.L.2003, 18(12), 481-487, at p.481.
[113] Steennot, ibid.
[114] ibid.
[115] EU Directive, preamble (2)

customers of the time needed for this to take place. [116] Steennot stated the reasons for the obligations as follows: firstly, to enhance the level of competition between financial institutions and, secondly, to reduce the time of execution, as this hinders efficiency within internal markets and, lastly, to increase transparency. [117]

The European Union aims for a single payment area, and promotes the efficiency and security of payment systems. [118] Enhancement of security procedures will protect the customer and boost his or her confidence in relation to all payment areas. [119] Consequently, in 1997 the European Union adopted the Council Directive 97/5 on Cross-Border Credit Transfers. The EU Directive has since attempted to harmonise the rules within the European Union in relation to cross-border credit transfer. Thereby, all the Member States implemented the EU Directive in their domestic law, as they were obliged to do so by 14 August 1999. [120]

### 2.4.2 The Rules of the EU Directive and an Unauthorised EFT

The Council Directive applies to cross-border credit transfers in euros or the currency of a member state of European Union, up to the equivalent of 50.000 Euro. Pursuant to Article (1)

> "[T]he provisions of this Directive shall apply to cross-border credit transfers in the currencies of the Member States and the ECU up to the equivalent of ECU 50.000 ordered by persons other than those referred to in Article 2 (a), (b) and (c) and executed by credit institutions or other institutions."

---

[116] ibid arts. 3 and 6.
[117] Steennot, note 112 supra at p. 483.
[118] ibid at p. 481.
[119] ibid.
[120] Report from the Commission to the European Parliament and to the Council: On the Application of Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, Brussels, 29.11.2002, COM (2002)663 final at p.10.

Moreover, Article 2 (f) has limited the scope of application of the Council Directive to credit transfers and denies other cross-border payments, for instance credit or debit card transactions. Furthermore, Article 2 (f) illustrates that a cross-border credit transfer occurs whenever the originator's bank and the beneficiary's bank are located in different Member States. Accordingly, the nationality of the originator and beneficiary or the place of residence is not relevant. Article 2 (f) states that 'cross-border credit transfer' means

> "a transaction carried out on the initiative of an originator via an institution or its branch in one Member State, with a view to making available an amount of money to a beneficiary at an institution or its branch in another Member State; the originator and the beneficiary may be one and the same person."

Article 2 (g) stipulates that the payment order could be issued in any form; accordingly, the Directive could be applied to electronic funds transfer transactions. Further, Article 2 (h) illustrates that it does not matter whether a consumer or professional gives the payment orders. Therefore, the Council Directive could be applied to wholesale EFT up to 50.000 Euros. Further, the Council Directive 97/5 on Cross-Border Credit Transfers applies to cross-border credit transfers between the Member States of the European Union, as well as to a credit transfer up to 50.000 Euro. Subsequently, the Council Directive does not apply to international credit transfers executed between Member States and Non-Member States, which makes the EU Directive cannot be applied to international EFT executed out the EU.

A thorough examination of the rules of EU Directive reveals that the EU Directive does not deal with the significant legal difficulties raised by EFT such as the problem of authenticated but unauthorised payment orders. The EU Directive has focused more on the transparency of information and terms, the time of executing the payment

order and the compensation for late or failed payment orders. Hooley argues that the EU Directive does not deal with crucial issues regarding EFT such as unauthorised payment orders. [121] For the purpose of this thesis, the EU Directive does not contain rules that regulate or govern the originator or the originator's bank's rights, duties or liabilities for unauthorised payment orders. Further, the EU Directive does not set out minimum standards for security procedures which should be implemented by the originator's bank. In the absence of rules regulating the above mentioned issues the originator and the originator's bank will be reluctant to use EFT. On one hand, because the originator's bank cannot predict its liability for authenticated but unauthorised payment orders and the scope of its liability for direct and consequential damages is not certain. Uncertainty of the liability for damages will be discussed in subsequent chapter. On the other hand, the originator is not protected from unfair contract terms that the originator' bank may include to exclude or limit its liability for fraudulent EFT.

The present author's view is that the EU Directive fails to deal with important problems in the context of EFT (unauthorised payment orders being one of the most significant). This imposes two important conclusions. Firstly, the EU Directive is not a comprehensive legal framework, and secondly, the EU Directive needs to be amended to regulate these problems. The present author's argument is that, given the fact that the EU Directive seeks to promote customer protection and improve the level of cross-border credit transfer services [122] and seeks greater competition and cost reduction, more should be done to achieve this. [123] These aims cannot be attained if there are no rules in place to govern the actions of the originator or the originator's

[121] Hooley, note 109 supra ar p. 389.
[122] Steennot, note 112 supra at p.481
[123] ibid.

bank with regard to their rights, duties and liabilities for unauthorised payment orders. These rights, duties and liabilities must be made more certain and predictable by adding rules to EU Directive regulating the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. Such rules should take into consideration the distinctive nature of the authentication of electronic payment orders, namely the problem of identity authentication and when an authenticated payment order is an authorised payment order or not.

## 2.5. THE UK REGULATIONS ON CROSS-BORDER CREDIT TRANSFER

### 2.5.1 The Scope of the UK Regulations

As mentioned above, the UK implemented the EU Directive by adopting the Cross-Border Credit Transfer Regulations 1999. [124] The UK regulations apply to cross-border credit transfers up to 50.000 Euro or its equivalent in another EAA currency and executes between the EU Member States.[125] Consequently, international wholesale EFT, which exceeds 50.000 Euros and is executed outside the EU Member States falls outside the remit of the regulations. [126] In June 1995, a report was published by the Select Committee on the European Communities which was appointed by the House of Lords (hereafter House of Lords' Committee) to examine the original proposal of the EU Directive. [127] The House of Lords' Committee was concerned with whether there is a need for a directive to regulate cross-border credit

[124] Hooley, note 109 supra at p. 387.
[125] UK regulations, Reg 2 (1), Ellinger, Lomnicka and Hooley, note 5 supra at p.503 and Hooley, ibid
[126] Hapgood, note 8 supra at p. at 330.
[127] House of Lords, Session 1994-1995 12t Report, Select Committee on the European Communities, Cross-Border Credit Transfers, with Evidence, 13 June 1995. (hereafter the House of Lords Committee report)

transfers or if it should be left to the banking sector to deal with. [128] The other issue the House of Lords' Committee was concerned with was whether high-value payments should be excluded from the scope of EU Directive - the Directive's remit, therefore, being limited to low-value payments only. [129] The House of Lords' Committee called for oral and written evidence on these issues from UK banking industry representatives, representatives of UK consumer groups and HM Treasury. [130] The House of Lords' Committee and these different sectors agreed that EU Directive should regulate cross-border credit transfers. [131] Cross-border credit transfers raise different problems which need to be addressed to improve transaction time and the standards of cross-border credit transfer, for instance, the problem of double charging and the subsequent redress arrangement. [132]

In terms of the EU Directive's scope, the House of Lords' Committee recognized that banking industry representatives were strongly against high-value payments being covered by the EU Directive. [133] The banking industry representatives argued *inter alia* that if the EU Directive's remit included high-value payments and became subject to the "money-back guarantee rule", the banking industry would be at high risk. [134] It would follow, therefore, that in incidents of fraud, the bank would be liable to refund a large amount of money to the customer pursuant to the "money-back guarantee rule". [135] Conversely, the representative of consumer groups did not argue that the EU Directive should cover the high-value payments. On the basis that the

---

[128] ibid.
[129] ibid.
[130] ibid
[131] ibid at p.8.
[132] ibid
[133] ibid
[134] ibid at p.8, oral evidence p.1-7.
[135] ibid at p.8.

consumer groups do not represent business customers, they were deemed to be "agnostic" on this issue. [136] However, the consumer groups were concerned that the scope of the EU Directive should be wide enough to cover individual payments for buying property. [137] The HM Treasury's view (representing the UK government) was that if there should be a limit to the EU Directive, it should be as high as possible, but declined to give a specific figure. [138] The HM Treasury's representative was aware that the EU Commission did not carry out any research into high-value payments, and believed that there might be problems if the payment order exceeded the level specified by the EU Commission. [139] Nonetheless, the HM Treasury decided to adopt the EU Council decision that the priority was to adopt legislation to protect the consumer and SMEs in the context of cross-border credit transfer. [140] Accordingly, the House of Lords' Committee agreed that the EU Directive should be confined to low-value payments. [141]

### 2.5.2 The Flaws of the UK Regulations in the Context of an Unauthorised EFT

Hooley confirmed that by adopting UK regulations, it was the first time the UK had a "statutory regime" regulating particular types of paper-based and electronic credit transfer. [142] The UK regulations (in correlation with the EU Directive) deal with issues related to the obligation to carry out the payment order on time, transparency of information before and after the payment order has been carried out and the

[136] ibid at p.8, oral evidence at p.21.
[137] ibid, oral evidence at p.22.
[138] ibid, oral evidence at p.25.
[139] ibid, oral evidence at p.27.
[140] ibid, oral evidence.
[141] ibid at p.8.
[142] Hooley, note 109 supra atp.387.

compensation for late or failed transfers. [143] The UK regulations do not contain rules to determine when the authenticated payment order is an unauthorised. They also fail to govern the parties' liabilities for authenticated but unauthorised payment orders. Hooley provides a convincing argument demonstrating why the UK regulations are not comprehensive enough. The regulations do not deal with important issues in the context of funds transfer [144] such as, an unauthorised payment order. [145] Thus, Hooley asserts that in the absence of rules within the UK regulations governing the problem of unauthorised payment orders, the common law would still apply. [146] The present author's view is that the UK Regulations fail to take into account the problem of identity authentication and its effects on an unauthorised payment order in the context EFT. The present author believes that the absence of rules regulating an authenticated but unauthorised payment order was the reason why the banking industry rejected high-value payments being included in the EU Directive. Through electronic means, the banks cannot determine if the person who sends the payment order is authorised to do so. The absence of these rules results in the banking industry being liable for unauthorised payments, irrespective of whether they are authenticated or not.

Accordingly, the present author argues that UK regulations need to be amended by adding rules to determine whether the payment order is authorised or not, taking into account the problem of identity authentication. Moreover, the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT need to be regulated. Regulating the originator and the originator's bank's relationship in the context of fraudulent EFT makes their rights, duties and liabilities more predictable

[143] Hooley, ibid.
[144] ibid at p.395.
[145] ibid at p.389.
[146] ibid.

and certain, and encourages them to use EFT to transfer money. Certainty and predictability can be achieved by adopting rules which contain the minimum standards of the UNCITRAL Model law rules which regulate authenticated but unauthorised payment order. [147] The UNCITRAL Model Law regulates the originator and the originator's bank's rights, duties and liabilities for unauthorised payment order. Accordingly, the originator and the originator's bank's rights, duties and liabilities are more predictable and certain. The UNCITRAL Model Law rules in the context of unauthorised EFT will be assessed in the next chapter.

Moreover, the limitation of the scope of the UK Regulations that are applied to funds transfer up to 50,000 Euro need to be removed, so the regulations would be applied to EFT regardless of its value. It is worth noting that some Member States have implemented of the EU Directive in their domestic law, they have extended the limits of their application beyond the EU Directive ambit. For instance, Denmark extended its legislation to cover countries out of the Member States and the EEA if these countries have equivalent rules. [148] Furthermore, Germany has extended the application of its domestic legislation to cover payment orders up to 75,000 Euro. [149] Some Member States such as Finland, Germany and Portugal apply the EU Directive to national credit transfers in addition to international credit transfers. [150] These examples show that EU Directive is flexible, and their limitations can be extended when they are implemented in domestic law as long as the extensions or variations do not contradict the objective of the EU Directive. Accordingly, the UK regulations are

[147] The UNCITRAL Model Law on International Credit Transfers 1992, art. 5.
[148] Report from the Commission to the European Parliament and to the Council: On the Application of Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, Brussels, 29.11.2002, COM (2002) 663 final, at p. 10.
[149] ibid.
[150] ibid.

able to be modified by regulating an authorised payment order and extend the scope of their application to cover EFT regardless of its value.

## 2.6.THE JACK COMMITTEE REPORT'S VIEW OF THE AUTHENTICATION SYSTEM

Although, it has been 20 years since the Jack Committee Report was published, it is still significant as it focuses on the legal problems arises in the context of EFT and the need for legal framework to govern and regulate such legal problems. However, the recommendations of the Jack Committee Report related to the problems arise in the context of EFT still have not been implemented in a legal framework regulates EFT transactions. Professor Jack who was the chairman of the committee states

> " [W]e addressed a number of our 83 recommendations to the Government in the they called for legislation. The Government largely accepted out recommendations and indicated their intention to legislate "as soon as other pressures on the Parliamentary timetable permitted." With one exception we still await legislation." [151]

In 1989, the UK Jack Committee Report emphasized that it is generally recognised around the world that authentication of instruction is one of the main problems relating to electronic funds transfer law and practice. [152] According to the Jack Committee Report, an authentication is "[M]eans of ensuring that a message or instruction in an EFT context comes from an authorised source; the most common example is the PIN." [153] More attention was focused on the standard of the security

[151] Robert Jack, " Still Waiting for Legislation," Scottish Banker, 1994, at p.16.
[152] Review Committee on Banking Services: Law and Practice, report by the Review Committee / Chairman: R.B. Jack, Vol. XLIX 622-630, 1989 at p.77 and p.82. (hereafter The Jack Committee report)
[153] ibid at p.viii.

procedures which should be applied to verify the source of the payment order to prevent error or fraud. The Committee Report demonstrated

> "...the difference between paper–based systems, authenticated by signature, and EFT where the signature is replaced by an electronic key. Because this less reliable means of authenticating a customer's instruction provides new scope for error and fraud, issues arise about the standards of security that should be applied at the design stage to customer-activated EFT system." [154]

In England, there is no statutory definition of security procedures in the context of EFT, and the required standard of security procedures should be implemented to authenticate payment orders. As the relationship between the bank and the customer in the context of authorised and authenticated payment orders is currently governed by agency law or mandate law, the question that arises is whether electronic security procedures are recognised and valid in common law to authenticate the payment order (as the handwritten signature). In other words, would the bank or the customer be able to depend on the security procedure (before the court) to prove that the payment order is an authenticated or an unauthenticated payment order? To answer this question in respect of the common law, a separate examination of the various forms of security procedures should be discussed in detail, to determine whether the common law recognises them as means of authentication. Therefore, the next section will be devoted to discussing the security procedure methods in use, namely passwords, user names and electronic signatures, to demonstrate whether they have legal validity in English law and their legal effects on the originator and the originator's bank's liabilities for an authenticated but an unauthorised payment order. The forthcoming pages conclude that the security procedures have legal validity as evidence under English law. However, the legal value of security procedures and their effect on the originator and the originator's bank's liability for authenticated but unauthorised is

[154] ibid at p.77.

not determined by particular rules and is left to the parties' agreement. This means that still the originator's bank will protect itself by stipulating unfair contract terms to escape liability for authenticated but unauthorised payment orders executed by a third party.

## 2.7. THE LEGAL VALIDITY AND FORMS OF SECURITY PROCEDURES IN THE CONTEXT OF EFT IN ENGLISH LAW

To boost bank and customer confidence in on-line transactions in general, and EFT in particular, both bank and customers must be sure that their personal data and the electronic communications are protected from third party interception, disclosure or manipulation. [155] Thus, on-line EFT raises two key issues: firstly, customer authentication, and secondly, the integrity of the payment orders. [156] In order to promote bank and customer confidence, the bank uses security procedures to be sure of the customer's identity and to ensure the integrity of any payment order. Accordingly, this section considers the form of security procedures, namely passwords, user names and electronic signature (hereafter e-signature); in particular symmetrical key encryption and public key encryption (the digital signature). The next section, examines the validity and the legal effect of these security procedures in England in the context of fraudulent EFT, as such security procedures are not regulated in any particular legal framework devoted to EFT.[157] The forthcoming pages will examine the legal validity and the effect of the security procedures on the originator and the originator's bank's liability for authenticated but unauthorised

[155] Azzouni, note 85 supra.
[156] Patricia Robertson and Patrick Goodall, "Internet Payments", Michael Brindle and Raymond Cox,(eds) 3rd ed, *Law of Bank Payments*, Sweet & Maxwell, London 2004 at p.266.
[157] The Jack Committee Report, note 152 supra at p. 25-26.

payment order under English law, namely the case law, the Electronic Communications Act 2000 and the Electronic Signature Regulations 2002.

### 2.7.1 Functions and Forms of Security Procedures

Before explaining the various forms of security procedures applicable to on-line EFT, it is appropriate to set out the general requirements of any security procedure. Firstly, there needs to be a system of confidentiality to protect the content of the exchanged information from being disclosed. [158] Secondly, to ensure identity authentication, the bank and the customer should be confident that they are communicating with the correct party before sending or accepting sensitive information. [159] The third requirement is data authentication which means that the security procedures are able to detect data manipulation such as insertion, deletion or substitution of the payment order details or, indeed, replay of the payment order by unauthorised parties.[160] Lastly, non-repudiation prevents the customer from denying the execution of the transaction. [161] Recognition of the above security requirements is important, as not all the electronic banking systems that provide security procedures have all of these functions.[162] Some electronic banking systems provide identity authentication but do not provide transaction authentication.[163] Claessens *et al* explain as follows:

> " [A]n important distinction should be made between entity and transaction authentication. Entity authentication means that the client authenticates when initiating a session with the bank. Transactions authentication means that individual transactions within this session are authorised by the client.

[158] Joris Claessens, Valentin Dem, Danny De Dock, Bart Preneel and Joos Vandewalle, "On the Security of Today's On-line Electronic Banking Systems", Joris Claessens, 2002 at p.5. http://joris.claessens.ws/pub/stoebs.pdf (obtained 5/6/2004)
[159] ibid.
[160] ibid.
[161] ibid.
[162] ibid at p.11.
[163] ibid.

> Depending on the authentication mechanism, transaction authentication can provide non-repudiation of single transactions, while entity authentication does not provide non-repudiation of transactions." [164]

Passwords in association with user name techniques (single-factor authentication), [165] are the premier identity authentication system [166] and banks in the UK still rely on them heavily and a lot more frequently than the electronic signature. [167] Password and user name techniques are popular for banks because of the low cost and ease of implementation and use. [168] Claessens states that "This password can be a PIN number or a character based password, and is often combined with a service account number that is not easy to guess." [169] There are two flaws in terms of password and user name techniques: they are used only for entity authentication, [170] and they are less secure.[171] Therefore, password and user name techniques are often combined either with a method of identity authentication [172] or with a transaction authentication system.[173] The combination of the passwords with another device the customer possesses or the customer has such as retina scanned and fingerprints recorded is a two-factor authentication.[174] Banks are encouraged by APACS to use two-factor authentication in online banking, as it is more secure than one-factor authentication. [175] The Association of Payment and Clearing Systems (hereafter APACS) announced

---

[164] ibid.
[165] Banks Need Two-Factor Authentication Urgently, Says Forrester, Out-Law. Com, New, 30/03/3005 at p. 1. (hereafter Banks Need Two-Factor Authentication).
http://www.out-law.com/page-5467
http://www.out-law.com (obtained on12/12/2005).
[166] M. Ford, "Identity Authentication and 'E-Commerce," (JILT), Issue 3,1998.
http://elj.warwick.ac.uk/jilt/98-3/ford.html (obtained 27/04/2004)
[167] Claessens, Dem, De Dock, Preneel and Vandewalle, note 158 supra at p. 11, Azzouni, note 85 supra at p.354 and Banks Need Two-Factor Authentication, note 90 supra at p.1.
[168] Claessens, Dem, De Dock, Preneel and Vandewalle, ibid and Azzouni, ibid.
[169] Claessens, Dem, De Dock, Preneel and Vandewalle, ibid.
[170] ibid.
[171] Ford, note 166 supra.
[172] ibid.
[173] Claessens, Dem, De Dock, Preneel and Vandewalle, note 158 supra at p. 11.
[174] Banks Need Two-Factor Authentication, note 165 supra at p.1.
[175] Banks Need Two-Factor Authentication, ibid.

that by the end of 2005, authentication standards for online banking would be issued.[176] Hence, all the major banks and financial institutions which are members of APACS should implement these authentication standards as standard. [177] The standard authentication will be the two-factor authentication system. The two-factor authentication will comprise a small device where a chip and PIN card is inserted. The PIN number entered and the device creates a one-time-only password which appears on the screen of the device. This password on the screen is used to authenticate the customer and enables him to access online banking. [178] Yet the standards of two-factor authentication have not been published by APACS. [179] However, in 2005 Lloyds announced a trial of 30,000 customers who were issued with a device which generates passwords. The customers use these devices to access their online banking and to engage in online transactions.[180] In addition to Lloyds, the Alliance and Leicester announced that in March 2006, two-factor authentication would be used for online banking transactions. [181] It is worth noting that the two-factor device has been used for many years in other countries such as the US, Sweden and the Netherlands.[182] Nonetheless, two-factor authentication is not an effective solution for

---

[176] "Online Banking Security Standard 'by the end of 2005'", ZDNet UK, News, 17/10/2005. (Hereafter online banking security standard 2005)
http://news.zdnet.co.uk/internet/security/0,39020375,39231006,00.htm
http://news.zdnet.co.uk (obtained 06/02/2006).
[177] ibid.
[178] ibid.
[179] "Two-Factor Authentication imminent from Alliance &Leicester," ZDNet UK, News, 28/02/2006. (Hereafter Alliance & Leicester)
http://news.zdnet.co.uk/internet/0,39020369,39254930,00.htm
http://news.zdnet.co.uk (obtained 06/03/2006).
[180] Lloyds TSB Tests Passwords-Generators, Out-Law. Com, News, 17/10/2005. (Hereafter Lloyds TSB)
http://www.out-law.com/page-6234
http://www.out-law.com (obtained on12/12/2005).
[181] Alliance &Leicester, note 179 supra.
[182] Lloyds TSB , note 180 supra.

online fraud, but it makes fraud harder to occur, as Trojan horses and phishing attacks can defeat two-factor authentication. [183]

Passwords and user names have been used for identity authentication in electronic banking services for a long time. [184] As a result of flaws in the password authentication system and the considerable growth of EFT (driven by the emergence and dramatic growth of the Internet, which gave rise to the Internet banking), the need for more secure and efficient security procedures to verify the entity and the payment order content has become a significant element in enhancing on-line banking. [185] An E-signature is one of the security procedures used to verify the identity of the sender, in addition to the integrity and authenticity of the payment order contents. [186]
E-signatures are "computer-based personal identities". [187] An E-signature can take different forms. The simplest one is the scanned image of a handwritten signature in a word processing document or a more advanced one like the biometric signature such as a retinal scan, which requires a special writing pad that records strokes and pressure. The most advanced method is called the digital signature, which uses public key cryptography. [188] The most widely used form of e-signature is the digital signature.[189] Angel has stated that the digital signature is used to perform three functions.

> " 1. Authentication - to authenticate the identity of the person who signed the data so it is known who participated in the transaction. 2. Integrity - to protect

[183] Online Banking security standard 2005, not 176 supra.
[184] Ford, note 166 supra.
[185] J. Angel, "Why Use Digital Signatures for Electronic Commerce?" Commentary (JILT), Issue 2, 1999 and Banks Need Two-Factor Authentication, note 90 supra at p. 1.
http://elj.warwick.ac.uk/jilt/99-2/angel.html (obtained 27/04/2004).
[186] ibid.
[187] C. Spyrelli, "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication," (JILT), issue 2, 2002.
http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html (obtained 27/04/2004)
[188] ibid and Angel, note 185 supra.
[189] Spyrelli, ibid.

> the integrity of the data so it is possible to know the message read has not been changed, either accidentally or maliciously.3. Non-repudiation, to allow it to be proved later who participated in a transaction so that it cannot be denied who sent or received the data." [190]

Digital signatures exist in two forms: the symmetrical public key and public key encryption. [191] A digital signature is dependant upon an encryption technique. [192] The encryption technique is defined as "the process of using algorithm, a mathematical rule, to translate a given message into a jumbled form which is then unreadable by anyone who does not have the correct mathematical rule to translate the message back into its original form". [193]

In symmetrical key encryption, the message is encrypted and decrypted with the same key. [194] The sender encrypts the message before sending it to the recipient, and then the message becomes unreadable. To transfer the message to readable form, the same key that was encrypted must decrypt it. The recipient who wants to decrypt this message must hold that key. [195] Robertson and Goodall rightly assert that symmetrical key encryption is suitable to be used in cases where the number of the participants in the same system is relatively limited and where customers can depend on each other to keep the shared key safe and undisclosed.[196] Hence, the message is decrypted and encrypted with the same key that makes the symmetrical key encryption more vulnerable to being disclosed. [197] The symmetrical public key is used between banks in the SWIFT system. [198]

---

[190] Angel, note 185 supra.
[191] ibid.
[192] ibid.
[193] Robertson and Goodall, note 156 supra at p.221.
[194] ibid at p.222.
[195] ibid at p.221-222.
[196] ibid at p.222.
[197] ibid.
[198] ibid.

Public key encryption consists of a pair of keys. One of the keys is called the public key, and the other is called the private key. [199] The public key is known by the public while the private key is only known by the sender. [200] Thus, the sender of an e-document can sign it and encode the data with the private key and send it to the recipient who in turn can decode it with the public key of the sender. [201] Where the public key can decrypt the message, the message is verified and sent by the sender, who has the private key. The private key is stored on the hard disc of the sender's computer or on a smart card. The sender gains access to the private key by typing a password or PIN. [202] Robertson and Goodall aptly argue that public key encryption is more difficult to break than symmetrical key encryption, because the message in public key encryption technique is encrypted and decrypted with different keys.[203] Therefore, the sender must keep the private key secret and must protect it from loss, theft, or unauthorised use, as any person who gains access to the private key can easily create a digital signature.[204]

Nonetheless, e-signature and encryption techniques do not provide sufficient evidence of the signatory's identity. Spyrelli [205] Robertson and Goodall [206] demonstrate this by asking: how can the participants be sure that the public key really does belong to the purported sender, since the private and public keys have no intimated connection with any person? On the other hand, how can participants be sure that the person who uses the public key to send the payment order is an authorised person? [207] It is

---

[199] ibid.
[200] Alistair Kelman, "An Introduction to Electronic Payment Mechanisms, Encryption, Digital signatures and Electronic Surveillance", Michael Chissick and Alistair Kelman, *Electronic Commerce, Law and Practice* 3rd ed, Sweet & Maxwell, London 2002 at p. 175.
[201] Spyrelli, note 187 supra.
[202] Angel, note 185 supra.
[203] Robertson and Goodall, note 156 supra at p.268.
[204] ibid.
[205] Spyrelli, note 187 supra.
[206] Robertson and Goodall, note 156 supra at p.272.
[207] ibid.

possible that a payment order issued by an unauthorised person gains unlawful access to the keys. As Robertson and Goodall emphasize:

> " [T]he use of a private key or other form of electronic signature to "sign" a document merely proves that the signer had had access to that key or signing device. Of itself, it cannot reliably prove the identity of the signer, far less whether, for example, the signer was duly authorised." [208]

Spyrelli [209] Robertson and Goodall [210] confirm that the Trusted Third Party (TTP) or alternatively Certificate Authority (CA) is a way to prove that a specific private or public key belongs to specific person. [211] Robertson and Goodall add that the TTP solution is highly regarded by the UK Government and the European Commission. [212] However, Robertson and Goodall explain that the TTP still does not help to identify whether the person who sends the payment order is authorised or not.[213] Hence, the next section will consider how the TTP works to demonstrate that it does give evidence of public or private key ownership but it does not help to authenticate the identity of the person who uses the public or the private key to send the payment order. This demonstrates that despite the existence of the TTP and the security procedures in English law being legally valid as an evidence to prove the execution of payment, the problem of identity authentication and its effect in determining whether the payment order is an authorised payment order or not is still not addressed. The remaining section of this chapter argues that an authorised and an unauthorised payment order in the context of EFT needs to be regulated by particular rules which take into consideration the distinct nature of the security procedures used to authenticate such payment orders.

---

[208] ibid.
[209] Spyrelli, note 187 supra.
[210] Robertson and Goodall, note 156 supra at p.273.
[211] Angel, note 185 supra.
[212] Robertson and Goodall, note 156 supra at p.273.
[213] ibid, at p.274.

## 2.7.2 The Trusted Third Party (TTP)

The TTP is a depositary for public and private keys. [214] For example, where a user wants to communicate with another party and does not know his public key, he can obtain it from the TTP. Moreover, the user might know the other person's public key but he wants to check that the public key he has been given by that party is in fact his public key and that he is a genuine individual or representing a genuine company.[215] The action of the TTP is similar to that of a notary act, which confirms that a specific person has signed a document after checking his identity, for example with his passport. [216] There are various methods which the TTP might use to check user identity. The TTP may issue a certificate after receiving an attestation from a third party which confirms the name, address and other personal information given in the online registration. The TTP might check user identity by asking the user to take the application to the notary. The notary will check the user's identification and confirm it. The TTP then issues a digital certificate which confirms that a particular company owns specific public and private keys. [217] The digital certificate is signed by the TTP using a private key. [218] The TTP could be the bank which provides the EFT service or a service provider. [219] When the customer sends a payment order to his bank, a digital signature and digital certificate are transmitted to the bank. Referring to the digital signature and a valid certificate, the bank can determine that the payment order

---

[214] ibid at p.273.
[215] Kelman, note 200 supra at p.180.
[216] Angel, note 185 supra.
[217] ibid, Robertson and Goodall, note 156 supra at p.273 and "Authentication in an Electronic Banking Environment", Federal Financial Examination Council. August 8, 2001 at p.6.
http://www.ffiec.gov/pdf/pr080801.pdf
http://www.ffiec.gov (obtained 24/04/2004)
[218] Angel, ibid and Robertson and Goodall, ibid
[219] Angel, ibid and Robertson and Goodall, ibid

has been executed by its originator. [220] However, this does not determine whether the person who sends the payment order is, in fact, an authorised person. The customer's private key is an electronic file, which is vulnerable and could be copied by intercepting the network or Internet. [221] Robertson and Goodall aptly confirm:

> "[O]f course, such a certificate [a digital certificate issued by the TTP] [222] merely ensures that one can reliably identify the authentic digital signature or public key used by X Ltd. It cannot guarantee that an unauthorised party has not got hold of that signature or the private encryption key and used it. The weak link in all these systems is ultimately the potential for fraud if the security of private key or other electronic signature device is compromised, enabling someone to masquerade undetectably as the authorised user." [223]

In conclusion, the TTP is not able to determine the identity of the person who sends the payment order. Accordingly, the TTP does not solve the problem of the parties' liability for authenticated but unauthorised EFT, which arises as a result of the application of the rules of agency law on EFT. Hence, the bank may include a term in the contract to exclude or limit its liability for an authenticated but unauthorised payment order. In such a case, the originator bears the whole liability for an authenticated but unauthorised payment order even if it is not the customer's fault or negligence or the implemented security procedures are unreasonable.

---

[220] Angel, ibid and Robertson and Goodall, ibid
[221] Angel, ibid and Robertson and Goodall, ibid
[222] The words in square brackets added.
[223] Robertson and Goodall, note 156 supra at p.274.

## 2.7.3 Validity of Security Procedures in English Law

Security procedures such as encryption, algorithm and passwords are recognised in both Article 4A in the USA and the UNCITRAL Model Law as acceptable and valid methods to authenticate EFT. [224] In England and the EU, such security procedures are still not recognised in particular rules relating to EFT as methods to authenticate EFT between the bank and the customer. As there is no comprehensive legal framework devoted to regulate EFT in UK and the EU. Therefore, a question may arise as to whether security procedures such as passwords and digital signatures, which are used to authenticate online EFT, are valid under English law and EU law. Moreover, the UK regulations and the EU Directive do not contain rules to determine the legal effect of security procedures on the originator and the originator's bank's liability for fraudulent EFT. In other words, would the originator and the originator's bank be liable for payment orders which are authenticated by these security procedures, as their liability for payment orders are signed by a handwritten signature? The UK has adopted the Electronic Communications Act 2000 and the Electronic Signature Regulations 2002. These laws regulate the legal validity of the security procedures, regardless of the type of transaction the security procedures are used for. Thus, these legislation could be applied to the security procedures used in EFT. The following pages focus on the validity and admissibility of passwords and digital signatures in English common law, the statute law and EU law in the context of EFT. To demonstrate that such security procedures are valid and admissible as evidence in the legal procedures in cases of dispute over EFT.

---

[224] Article 4A-201, The UNCITRAL Model Law article 2 (i) and Carl Felsenfeld, "Article 4A of the United States Uniform Commercial Code", Walther Hadding and Uwe H. Schneider (eds), *Legal Issues in International Credit Transfers*, Duncker & Humblot, Berlin 1993 at p. 351.

## (a) What Is S Signature?

There is no statutory definition for the signature in England which might help to determine whether passwords or electronic signatures are deemed to be signatures or not. [225] Neither the Interpretation Act 1978 nor the statutes, (which require signatures for the validity of transactions) contain a definition of "signature".[226] However, case law for many years has drawn an analogy between the manuscript signature and other forms of authentication. [227]

Courts in the UK have adopted two approaches to determine the validity and efficacy of a signature - the "form approach" and the "function approach". [228] The "form approach" is used to determine whether the signature has the required form, for example, the name of the signer or his initials. Meanwhile the "function approach" is used to determine the function of a signature. It then examines other signature methods or techniques to see if they achieve the same functions. Thus, any signature method or technique performing the same function is deemed to be a signature. [229]

Robertson and Goodall have stated as follows

> "[I]f a functional approach is taken to what constitutes a signature there are strong arguments for recognising electronic signatures as true equivalents for all legal purposes: an electronic signature created using the type of techniques discussed above [asymmetrical key encryption and public key encryption] [230] is much more difficult to forge and, in that sense, more reliable a proof of identity than a handwritten signature." [231]

---

[225] Chris Reed, "What is a Signature?" (JILT), Issue 3, 2000. http://elj.warwick.ac.uk/jilt/00-3/reed.html/
[226] ibid.
[227] ibid.
[228] ibid.
[229] ibid.
[230] The words in square brackets added.
[231] Robertson and Goodall, note 156 supra at p.279.

Reed stated that the electronic signature would be valid if it performs the functions of a signature irrespective of the form it takes. [232] Angel rightly viewed that the job of a signature is to perform three functions: authenticity, integrity and non-repudiation regardless of the form of the signature. As passwords and electronic signatures perform these functions they should be valid. [233]

The functional approach of signature validity has been adopted in *Goodman v. J Eban Ltd.*[234] In this case, the Court of Appeal decided by a majority to recognise a signature produced by means of a rubber stamp as a valid signature. Sir Raymond Evershed MR said

> "Indeed, if reference is made to the Shorter Oxford English Dictionary, it will be found that the primary meaning of the verb "to sign" is not confined to actual writing with a pen or pencil. The word in origin appears to have related to marking with the sign of the cross. But the latter meaning included "(2) To place some distinguishing mark upon (a thing or a person)" and "(4) To attest or confirm by adding one's signature; to affix one's name to (a document, etc.). It follows, then, I think, that the essential requirement of signing is the affixing, either by writing with a pen or a pencil or by otherwise impressing on the document, one's name or "signature" so as to authenticate the document."[235]

The judgement illustrates that the efficacy and validity of a signature method is examined with reference to the functions it performs. The signature method, which provides evidence of the document's authentication by the purported signatory, should be a valid signature.[236] Reed has stated that the courts, according to the case law,[237]are ready to accept any signature that provides evidence of, firstly, the identity

---

[232] Reed, note 225 supra.
[233] Angel, note 185 supra.
[234] *Goodman v. J Eban Ltd,* [1954] 1 Q.B. 550.
[235] *Goodman v. J Eban Ltd,* ibid at p. 558.
[236] Reed, note 225 supra.
[237] See Goodman v. J Eban Ltd, note 234 supra, followed by Firstpost Homes Ltd v Johnson,[1995] 1 W.L.R. 1567.

of the signatory, secondly, the signatory's intention to sign and thirdly, the signatory's intention to adopt the document. [238]

The digital signature provides the functions of the signature. [239] Firstly, the electronic signature authenticates the identity of the person who signed the data, so it is known that the sender or the person who is authorised possesses the password or the private key. Secondly, it protects the integrity of the data and confirms that the message's contents have not been changed, either "accidentally or maliciously". [240] Lastly, non-repudiation allows it to be proved later who sent or performed the transaction so the person who sent or received the funds transfer cannot deny his participation. [241] Subsequently, security procedures such as passwords, PIN and e-signature, which are used to execute payment orders, are valid in England under common law, according to the functional approach recently adopted by the case law. However, the UK enacted two different types of legislation regulating e-signature - firstly, the Electronic Communications Act 2000 and, secondly, the Electronic Signature Regulations 2002. These legislation are an implementation of the EU Electronic Signature Directive (EC1999/93).[242]

---

[238] ibid.
[239] Angel, note 185 supra.
[240] ibid.
[241] ibid.
[242] The Electronic Signatures Directive 1999/93/EC on a Community framework for electronic signatures, OJ L13 p. 12, 19 January 2000 (hereafter EU Electronic Signature Directive), Justine Harrington, "U.K. and European Legislative Initiatives regulating Electronic Commerce", Michael Chissick and Alistair Kelman, *Electronic Commerce, Law and Practice* 3rd ed, Sweet & Maxwell, London, 2002 at p. 309 and J. Murray, "Public Key Infrastructure Digital Signatures and Systematic Risk", (JILT),Issue 1, 2003.
http://elj.warwick.ac.uk/jilt/03-1/murray.html

## 2.7.4 The EU Electronic Signatures Directive

In 2000, the Electronic Signatures Directive (EC1999/93) was enacted by the European Union. The aim of the Directive was to strengthen confidence and general acceptance of electronic signatures. According to the preamble of the Electronic Signature Directive (EC1999/93) the diversity in the rules with respect to the legal recognition of electronic signatures may hinder the free movement of goods and services in the internal market. [243] Accordingly, the Directive sets out the legal framework for e-signature and the certification authority services. [244]

The Directive classified e-signatures as a simple e-signature and an advanced e-signature.[245] Article 2 (1) states that e-signature means " ...data in electronic form which is attached to or logically associated with other electronic data and which serve as method of authentication." Taylor has stated that "this definition could thus include authentication techniques other than digital signature, such as biometric and retina scans". [246] The advanced e-signature pursuant to Article 2(2) means

> " an electronic signature which meets the following requirements:
> (a) it is uniquely linked to the signatory;
> (b) it is capable of identifying the signatory;
> (c) it is created using means that the signatory can maintain under his sole control; and
> (d) it is linked to the data to which it relates in such a manner that any subsequent change of data is detectable."

The advanced e-signature is an e-signature issued by the TTP and provides the customer with certificates to identify and confirm his ownership of the signature. [247]

---

[243] The preamble of The Electronic Signatures Directive 1999/93/EC on a Community Framework for Electronic Signatures.
[244] ibid Article (1).
[245] Reed, note 225 supra and Spyrelli, note 187 supra.
[246] Mark Taylor, "Electronic Signatures and Admissibility of Computer Records", Paul Anning, Emily Reid and Heather Rowe (eds), *E-Finance: Law and Regulation,* LexisNexis, London, 2003 at p.392.
[247] Reed, note 225 supra and for an analysis of what the TTP and the e-signature are, see sections 2.7.1and 2.7.2 of this chapter.

Hence, EU Directive recognises both types of e-signature, whether it be registered with the TTP or the simple one, which does not need registration with TTP such as passwords.

The Directive defines the signatory as the person who holds the signature-creation device (the public key and the private key). This signatory could be a natural or legal person, who acts on his behalf or on behalf of another natural or legal person. [248]

The Directive ensures that the legal validity and efficacy of an advanced e-signature is equivalent to the handwritten signature.[249] Article 5 of the Directive ensures the legal validity and effectiveness for simple and advanced e-signatures. In regards to the simple e-signature, according to Article 5 (2), the Member States must ensure, in their domestic law, that the validity and admissibility of e-signatures are not denied merely because they are in e-form, or not certified. [250] Nonetheless, the Member States could refuse to recognise the e-signature for reasons other than the reasons mentioned in Article (5). [251]

Under Article 5 (1), only the advanced e-signature is valid and admissible in legal procedures and given the same state as the handwritten signature. This is provided that the advanced e-signature satisfies the legal requirements for a signature in terms of an e-document, in the same way that the handwritten signature satisfies the legal requirements in paper-based transactions.[252] An advanced e-signature satisfies the legal requirements upon a certificate issued by a Certification Authority, which

[248] EU Electronic Signature Directive , Article 2 (3).
[249] ibid, Article 5.
[250] ibid Article 5 (2).
[251] Reed, note 225 supra.
[252] Angel, note 185 supra and Reed, ibid. For an analysis of what an e-signature is, see section 2.7.1 of this chapter.

verifies the signatory's data and confirms his identity and that the e-signature was executed by "secure signature creation device". [253]

## 2.7.5 The EU E-Signature Implementation in the UK

To implement the EU E-signatures Directive, the UK enacted the Electronic Communications Act 2000. [254] The purposes of the Electronic Communications Act 2000 were "to make provision to facilitate the use of electronic communications and electronic data storage". [255] Moreover, the Electronic Communications Act regulates the electronic signature and the services of the Certificate Authority and grants the legal validity for e-signature in legal procedures. [256] In the Electronic Communications Act, admissibility and legal validity have been granted to the e-signature. [257] Section 7 (1) provides as follows:

> "(1) in any legal proceedings
> (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
> (b) the certification by any person of such a signature,
> shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication data."

The provisions of the Electronic Communications Act 2000 deal with all methods of electronic security procedures, and are used to determine the authenticity or integrity of electronic communications. [258] Section 7 (2) defines electronic signature thus:

> " [F]or the purposes of this section an electronic signature is so much of anything in electronic form as

[253] ibid. For more information about the TTP see section 2.7.2.
[254] Harrington, note 242 supra at p.309.
[255] The Electronic Communication Act 2000, ch. 7.
[256] Reed, note 225 supra.
[257] The Electronic Communication Act 2000, section 7 (1).
[258] Claire Coleman, "Electronic Signatures in Banking", F & C.L.2001, 3(5), 1-3, at p.2.

(a) in incorporated into or otherwise logically associated with any electronic communication or electronic data, and
(b) purports to be so incorporated or associated for the purposes of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both."

Taylor confirms that the electronic signature in the Electronic Communications Act is defined in broad enough terms that anything in electronic form used with electronic communications and data to authenticate these communications or data is covered. [259]

Taylor explained according to section 7 (1) that in the UK, an e-signature is admissible evidence in legal proceedings in terms of the authenticity and integrity of any electronic communication or data.[260] However, Taylor opines that the Electronic Communications Act does not determine the legal effect of electronic signatures and it is for the court's discretion to decide the legal weight of electronic signatures according to the type of transaction. Robertson and Goodall confirm:

> " [T]he Electronic Communications Act 2000 is, however, silent on the legal effect of electronic signatures, leaving it to the Courts to assess the evidential weight to be attributed to a given type of electronic signature and whether an electronic signature is capable of satisfying a legal requirement for a signature in a particular statutory context." [261]

Accordingly, the present author argues that if these opinions are taken to their logical conclusion, the implication is that, on one hand the e-signature is admissible evidence in the context of EFT. On the other hand, the legal effect of electronic signatures on the originator and the originator's bank's liability for unauthorised payment orders is not confined and is, therefore, left to the court's discretion. There are no specific rules within a statute or regulations that apply to EFT; therefore it is for the court to evaluate the weight of e-signatures. In such cases, the court may depend on the originator and the originator's bank's agreement to evaluate the effect of an e-

[259] Taylor, note 246 supra at p.388.
[260] ibid.
[261] Robertson and Goodall, note 156 supra at p.278.

signature. The banks in these agreements stipulate terms, which exclude or limit their liability for authenticated but unauthorised payment orders issued by a third party. Consequently, the originator might be liable for authenticated but unauthorised payment orders where the originator's bank does not implement reasonable security procedures. In terms of unauthorised payment orders, the Electronic Communications Act does not solve the problem of identity authentication and its effects on the originator and the originator's liability for authenticated but unauthorised payment orders. If a legal effect is given to electronic signatures in the context of EFT, the originator who is not at fault or negligent might be liable for authenticated but unauthorised payment orders issued by a third party if the bank concerned implemented unreasonable security procedures. In contrast, if a legal effect is not given to the electronic signature, this would make the originator's bank liable for authenticated but unauthorised payment orders issued by one of the originator's employees or a third party as a result of the originator's fault or negligence. Thus, the originator and the originator's bank's liability for authenticated but unauthorised payment orders is still uncertain and unpredictable as it is for the court to decide to give legal effect to electronic signatures.

The present author argues that rules must be adopted to confine the originator and the originator's bank's liability for authenticated but unauthorised payment orders by proportioning the liability for such transactions. Further, such rules should impose a duty on the originator's bank to implement minimum standards of security procedures to authenticate payment orders. The present author argues that the rules of the UNCITRAL Model Law and Article 4A relating to authenticated but unauthorised payment orders should be taken in consideration when adopting rules governing

authenticated but unauthorised payment orders. A thorough examination revealing why the rules of UNCITRAL Model Law and Article 4A should be taken into consideration will be conducted in Chapter three.

Finally, the UK has implemented the EU Electronic Signature Directive by adopting the Electronic Signature Regulations 2002, which came into force in March 2002. [262] The UK Regulations mirrored the EU E-signature Directive definition of the e-signature[263] and implemented the Directive's requirements for supervising the Certificate Authority providers' services.[264] E-signature Regulations do not state clearly the legal effect of an e-signature and leave it to the court's discretion to give legal effect to electronic signature (as with the Electronic Communications Act). Therefore, it would be difficult to say how the E-Signature regulations were helpful in determining the originator and the originator's bank's liability for authenticated but unauthorised EFT.

In conclusion, in England and the EU, the e-signature is admissible as evidence in legal procedures in cases of dispute over EFT. However, the legal effect of e-signature on the originator and the originator's bank's liability for authenticated but unauthorised payment orders is left to the court's discretion. Accordingly, the originator and the originator's bank's liability for authenticated but unauthorised payment orders is still governed by rules of contract law and agency law. Thus, the EU E-signatures Directive 2002, the Electronic Communications Act 2000 and the E-signature Regulations 2002 do not provide solutions for the problem of identity

[262] Murray, note 242 supra.
[263] Electronic Signature Regulations 2002, no.318, s.2 interpretation.
[264] ibid s. 3 supervision of certification – service-provider.

authentication and its legal effects on the originator and the originator's bank's liability for authenticated but unauthorised EFT.

## 2.8. CONCLUSION

In the UK, in the absence of particular rules regulating wholesale EFT, agency or mandate law applies to determine the authenticity of a payment order and to determine whether the payment order is authorised or not. [265] This gives rise to the problem of identity authentication in EFT, since, in EFT, the bank receives the customer's mandate through an electronic access device (e.g. Internet or computer terminal). [266] Thus, the bank is exposed to the risk of being liable for an authenticated payment order, even if an unauthorised person executes it. [267] Therefore, to avoid accountability, the bank excludes or limits itself from the liability for unauthorised payment orders. [268] Hence, the bank allocates the risk to the customer by stipulating such conditions in its agreement, regardless of the possible fact that an unauthorised payment order has been executed by a third party or has occurred as a result of the inefficiency of their security procedures. [269] Furthermore, the EU E-signatures Directive 2002, the Electronic Communications Act 2000 and the E-signature Regulations 2002 do not provide solutions for the problem of identity authentication and its legal effects on the originator and the originator's bank's liability for authenticated but unauthorised EFT.[270]

---

[265] *Fielding v Royal Bank of Scotland Plc*, note 53 supra, para 56.
[266] Hapgood, note 8 supra at p. 336 and for more detail about the problem of identity authentication see section 2.3.1 of this Chapter and section 1.2.5 of Chapter one.
[267] Cranston 2002, note 59 supra at p. 140-141, Cranston 1993, note 59 supra at p.224 and Arora 1997, note 38 supra at p.134.
[268] Azzouni, note 85 supra at p.360.
[269] ibid.
[270] For more details about these legislation and their legal effects see section 2.7.4 and 2.7.5 of this chapter.

The UNCITRAL Model Law contains rules to solve the above-mentioned problems. The UNCITRAL Model Law contains rule apply to electronic payment orders authenticated by security procedures. [271] These rules, taking into consideration the method used to authenticate the payment order, are different and incomparable to the methods used in paper-based payment orders. [272] Similarly, in the US the rules of Article 4A regulate the originator and the originator's bank's rights, duties and liability in situations where a payment order is an authenticated but an unauthorised payment order. [273] The present author argues that in England and the EU specific rules need to be adopted to regulate the originator and the originator's bank's rights, duties and liabilities for an authenticated but unauthorised payment order. Such rules should adopt the minimum standards of the UNCITRAL Model Law and Article A4 in the context of an authenticated but unauthorised payment order. Thus, the next chapter considers the originator and the originator's bank's rights, duties and liability for an authenticated but unauthorised payment order under the UNCITRAL Model Law and Article 4A. The Chapter will demonstrate that the parties' rights and liabilities for such payment orders are more predictable and certain under the UNCITRAL Model Law and Article 4A than under the rules of agency law and contract law.

[271] UNCITRAL Model Law, Article 5 (2) to 5 (4).
[272] ibid.
[273] Article 4A, Section 202.

# CHAPTER THREE

# EXAMINTION OF THE UNCITRAL MODEL LAW AND ARTICLE 4A IN THE CONTEXT OF UNAUTHORISED EFT

## 3.1. INTRODUCTION

As indicated previously, the large amount of money transferred through EFT to settle international payments, the incorporation of communication technology and banks' desire to offer competitive funds transfer services,[1] together stimulate the banks to transfer money effectively, at high speed and low cost. [2] The lack of particular rules in delineating the originator and the originator's bank's rights, duties and liabilities in the context of unauthorised EFT expose the originator and the originator's bank to unpredictable and uncertain liability for unauthorised EFT. [3] As Thevenoz confirms:

> "[T]he absence of a well-defined body of law applicable specifically to paperless funds transfer, both in Common Law and in several Civil Law countries, has created much uncertainty, especially with regard to the finality and revocability of a payment order, and the allocation of losses in case of fraud, error and insolvency. These uncertainties became a major concern to banks experiencing the lack of a statutory "safety net" as soon as some of their largest clients refused to accept disputed contractual provisions allocating losses." [4]

---

[1] Uwe H. Schneider and Darmstadt/Maniz, "The Uniform Rules for International Credit Transfers under the Uncitral Model Law," Walther Hadding, and Uwe H. Schneider (eds), *Legal Issues in International Credit Transfers*, Duncker & Humblot, Berlin 1993 at p.454 and Bhala, Raj, " International Payments and Five Foundations of Wire Transfer Law," Essays in International Financial & Economic Law No, 2, International Finance and Tax Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, University of London, in cooperation with the London Centre for International Banking Studies and the London Institute of International Banking, Finance and Development Law, London, 1996 at p. 6-7.

[2] Schneider and Maniz ibid and Bhala 1996, ibid.

[3] Schneider and Maniz ibid and Bhala 1996, ibid.

[4] Luc Thevenoz, "Error and Fraud in Wholesale Funds Transfers: U.C.C. Article 4A and The UNCITRAL Harmonization Process," 42 Ala. L. Rev.881, Winter, 1991, at p.883.

One of the key thrusts to adopting the UNCITRAL Model Law and Article 4A is to demarcate the parties' rights, duties and liabilities for fraudulent EFT. [5] Consequently, the UNCITRAL Model Law and Article 4A devoted rules apply to unauthorised EFT.[6] These rules allocate liability between the originator and the originator's bank by taking into consideration the security procedures used to authenticate electronic payment orders. [7]

The purpose of this chapter is to assess the rules of the UNCITRAL Model Law, and how Article 4A applies to an authenticated but unauthorised EFT. This chapter evaluates whether those rules lead to predictability and certainty in the originator and the originator's rights, duties and liabilities for an authenticated but unauthorised EFT. It will conclude that the rules of the UNCITRAL Model Law and Article 4A delineate the originator and the originator's bank's rights, duties and liabilities for an authenticated but unauthorised EFT. Accordingly, these rules lead to greater predictability and certainty in the parties' rights, duties and liabilities for an authenticated and unauthorised EFT than is the case under English common law. Section 3.2 will examine the rules of the UNCITRAL Model Law by starting with the background and the history behind adopting the UNCITRAL Model Law. It then conducts an assessment of the rules of the UNCITRAL Model Law, as applied to unauthorised EFT, to demonstrate that the originator and the originator's bank's rights, duties and liabilities for authenticated but unauthorised payment order are predictable and certain. Lastly, this section will demonstrate the standard of the authentication system should be implemented by the originator's bank to authenticate payment orders according to UNCITRAL Model Law. Then Section 3.3 of this

[5] ibid, at p. 900.
[6] ibid.
[7] ibid, at p. 935-936.

chapter is devoted to analysing the rules of Article 4A, as applied to an authenticated but unauthorised EFT. This section outlines the driving forces behind adopting Article 4A in the US, and demonstrates that by applying the general principles of contract law, agency law and case law is not adequate in dealing with unauthorised EFT. Furthermore, section 3.3 examines the rules of Article 4A as applied to authenticated and unauthorised payment orders to elaborate on the fact that the originator and the originator's bank liability for authenticated but authorised EFT is more predictable and certain. Finally, section 3.3 evaluates the rules of Article 4A, which determine the originator's bank duty to implement "commercially reasonable" security procedures to authenticate payment orders issued by the originator. To demonstrate the effects of this rule on the originator and the originator's bank liability for authenticated but unauthorised payment order. This chapter concludes by arguing that the rules of the UNCITRAL Model Law and Article 4A lead to predictability and certainty in the above-mention parties' rights, duties and liabilities in such transactions.

## 3.2. THE UNCITRAL MODEL LAW AND UNAUTHORISED EFT.

### 3.2.1 The UNCITRAL Model Law

In 1982 the Secretary General of the UNCITRAL prepared a report which focused on legal issues in respect of international EFT. [8] According to the report, there were legal problems peculiar to international EFT, namely the finality of payment and its consequences and the liability for loss as a result of delay or incorrect payment instructions [9] such as fraud and error. Further, there was a problem with the legal validity of payment orders kept in electronic forms. [10] The focus of this thesis is on the originator and the originator's bank's rights, duties and liabilities in the context of fraudulent EFT. In 1986 the UNCITRAL decided to establish a Working Group with the task of drafting a model law on international credit transfer, to solve the former legal issues. [11] The UNCITRAL Study Group on International Payments (hereafter the Study Group) was appointed to prepare the draft of the model law. [12] In 1986, the Report of the Secretary –General in respect of the preparation of the UNCITRAL Model Law has stated that the use of electronics has led to changes in banking procedures therefore new legal rules were required. [13] Furthermore, the report pointed out that some of the rules that apply to paper-based funds transfer should be

---

[8] Electronic Funds Transfer: Report of the Secretary-General: Electronic Fund Transfer, UNCITRAL Yearbook Volume XIII: 1982 (A/CN.9/SER.A/1982) p.272 at p. 275. (Hereafter Report of the Secretary General 1982)
http://www.uncitral.org/pdf/english/yearbooks/yb-1982-e/yb_1982_e.pdf (obtained on 22/06/2004)
[9] ibid at p.276.
[10] ibid.
[11] Electronic Funds Transfers, Report of the Secretary- General (A/CN.9/278), Yearbook of the UNCITRAL, 1986, Vol. XVII, at p.81. (Hereafter Report of the Secretary General 1986)
http://www.uncitral.org/pdf/english/yearbooks/yb-1986-e/yb_1986_e.pdf (obtained on 12/12/2005).
[12] ibid.
[13] ibid at p.82.

reconsidered in the light of the new banking and legal environment, [14] and has emphasised that

> "...electronic funds transfers have developed in a partial legal vacuum... . Although basic banking procedures are the same whether funds transfer is made by paper-based means or electronically, and as result of many rules governing paper-based funds transfers can be applied to electronic funds transfer with appropriate results, many other rules should be reconsidered in the light of the new banking and legal environment. Decisions should be made as to such matters as the legal value to be given to the authentication of an electronic funds transfer instruction, the right of a bank to debit an account when the customer denies having issued an electronic funds transfer instruction and there is no independent paper record, and the frequency at which and the means by which a bank must inform a customer of debits or credits to his account and the obligation of the customer to inform the bank of errors." [15]

The above-mentioned report is in line with, and supports the present author's argument that EFT raises legal problems which cannot be solved by the application of rules applied to paper-based funds transfer. The report showed that the integration of electronic means to carry out funds transfer has given risen to specific legal problems that must be regulated, for example, the legal validity of the security procedure, and when the payment is an authorised payment order or not. The next section demonstrates how the rules adopted by the UNCITRAL Model Law can solve these problems.

In 1992 the Commission adopted the UNCITRAL Model Law on International credit transfer. [16] Under Article 2 (a) of the UNCITRAL Model Law, credit transfer means:

> "[T]he series of operations, beginning with the originator's payment order, made for the purpose of placing funds at the disposal of a beneficiary. The term includes any payment order issued by the originator's bank or any

---

[14] ibid.
[15] ibid.
[16] Report of The UNCITRAL on the Work of its Twenty-Fifth Session, Draft Model Law on International Credit Transfers, Yearbook Vol. XXIII 1992, at p. 13-14. ( hereafter Commission Report 1992)
http://www.uncitral.org/pdf/english/yearbooks/yb-1992-e/yb_1992_e.pdf (obtained on 12/12/2005).

intermediary bank intended to carry out the originator's payment order. A payment order issued for the purpose of effecting payment for such an order is considered to be part of a different credit transfer."

Whilst, the driving force behind adopting the UNCITRAL Model Law was to solve the problems related to EFT, the UNCITRAL Model Law applies to both paper-based and electronic credit transfer. [17] The Study Group decided to incorporate both types of credit transfer, based on the fact that the payment orders might be issued by using different method such as paper-based and electronic means. [18] As Bergsten rightly argues " [I]n any case, the provisions governing high-speed electronic credit transfer should be the same provisions governing credit transfers made by paper, magnetic tape or telex except where technology requires a difference." [19] The present author agrees with Bergsten because the difference between EFT and paper-based funds transfer is the method used to issue the payment order. In EFT the payment order is authenticated by using electronic security procedures, whereas in paper-based funds transfer, the payment order is authenticated by verifying the originator's hand-written signature. Therefore, some aspects of EFT, where the electronic means involve and affect the bank-customer's rights, duties and liabilities, should be regulated by particular rules: for instance, when the payment order is an authorised payment order with the existence of the problem of identity authentication in EFT and subsequently the bank-customer liabilities for authenticated but an unauthorised payment order. Bergsten explains that the payment order issued electronically is authenticated by electronic means, as it cannot be signed. The difference in authentication method

[17] Eric E. Bergsten, " A payments Law for the World: UNCITRAL Model Law on International Credit Transfers," Robert C. Effros, (ed), *Payment Systems of the World*, Oceana Publications, New York, London, 1996, at p.428.
[18] ibid.
[19] ibid at p.429.

raises the question of whether the rules applying to a forged signature should be applied to unauthorised electronic payment orders. [20]

The UNCITRAL Model Law is a guide for national legislators, to be adopted in their domestic law. [21] The UNCITRAL Model Law is a legal framework that includes rules governing the entire transaction of funds transfer: namely, the relationship between the originator and his bank; the relationship between the beneficiary and the beneficiary's bank or the intermediary bank; and the inter-bank relationship. [22] The UNCITRAL Model Law regulates the former parties' rights, duties and liabilities in the context of EFT. [23] The focus of this thesis is on the rules of the UNCITRAL Model Law that regulate the originator and the originator's bank's rights, duties and liabilities in the context of fraudulent EFT. The next section will examine the rules of the UNCITRAL Model Law as applied to determine whether the payment order is authorised or not. It will further demonstrate that the UNCITRAL Model Law has adopted rules applying specifically to the methods used to authenticate electronic payment orders to determine the parties' rights, duties and liabilities for authenticated but unauthorised EFT. Such rules lead to more predictability and certainty in the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT.

[20] Eric E. Bergsten, "UNCITRAL Model Law on International Credit Transfer," J.I.B.L. 1991, 6(7), 276-283, at p. 277-278.
[21] Schneider and Maniz, note 1 supra at p. 455.
[22] ibid at p.454.
[23] ibid.

### 3.2.2 Unauthorised EFT under the UNCITRAL Model Law.

EFT involves the problem of identity authentication that makes the bank unable to differentiate between an authorised and an unauthorised payment orders. [24] In view of this, the UNCITRAL Model Law contains different rules for payment orders, to determine whether the payment order is an authorised one or not, according to the methods used to authenticate the payment orders. [25] However, Article 2 (i) of the UNCITRAL Model Law defines authentication (security procedures) as

> " a procedure established by agreement to determine whether a payment order or an amendment or revocation of a payment order was issued by the person indicated as the sender."

The above definition is wide enough to encompass a handwritten signature and security procedures [26] such as handwritten signature, passwords and electronic signature. [27] The Commission of the UNCITRAL Model Law (hereafter the Commission) rejected the suggestion that a handwritten signature should not be included within the definition of authentication. The Commission demonstrated that even though a hand written signature is not a "commercially reasonable" way to authenticate large value credit transfer, it might be "commercially reasonable" for low value credit transfer. [28] This is understandable because the UNCITRAL Model Law has been adopted to regulate electronic and non-electronic funds transfer, and accordingly, the hand written signature cannot be excluded.

---

[24] Bergsten 1996, note 17 supra at p. 443.
[25] UNCITRAL Model Law Article 5 (1), (2), (3) and (4).
[26] Report of The UNCITRAL Commission on the Work of its Twenty-Fourth Session, Draft Model Law on International Credit Transfers, Yearbook Vol. XXII 1991, p.5-38 at p.12, para 69-70. ( hereafter Commission Report 1991) http://www.uncitral.org/pdf/english/yearbooks/yb-1991-e/yb_1991_e.pdf (obtained on12/12/2005).
[27] See Chapter two section 2.7.1. for more details on the different types of security procedures.
[28] Commission Report 1991, note 26 supra at p.12, para 70.

Instead, the Commission decided to dedicate a rule to apply to a handwritten signature payment, in order to distinguish from the rules applying to payment orders authenticated by procedures which are not a mere comparison to a handwritten signature. [29] Article 5 of the UNCITRAL Model Law is divided two-fold; Article 5 (1) is applied to a payment order authenticated by a handwritten signature, while Article 5 (2) to 5 (4) is applied to a payment order where the authentication procedures used are not a "mere comparison of signature." [30] According to Article 5(1) when the payment order is authenticated by a comparison of the handwritten signature of the originator, the originator is only liable for authorised payment orders.[31] Hence, the bank can debit the customer's account, depending on an authorised payment order, issued either by the customer or by a person who is authorized by the customer to do so. [32] Patrikis *at el* state that Article 5(1) does not provide any limitations or qualification for the authority.[33] Therefore, the rules of agency law determine whether the person who issues the payment order is authorised to do so or not. [34] Such authority could be actual authority or apparent authority.[35] Bergsten has explained that under UCITRAL Model Law, the "bank bears the risk of forgery" when the authentication of payment order is a "mere comparison to a handwritten signature." [36] Indeed, under Article 5(1) of the UNCITRAL Model Law, the traditional rule still applies in terms of the payment order authenticated by a

---

[29] ibid, at p.12 paras 69-70, p. 17, paras 107-108.
[30] UNCITRAL Model Law Article 5 (2).
[31] International Credit Transfer: Comments on the Draft Model Law on International Credit Transfer: Reports of the Secretary-General (A/CN.9/346), UNCITRAL yearbook, vol. XXII, 1991, p.52-102 at p. 64 ( Hereafter Report of the Secretary-General 991) and Bergsten 1996, note 17 supra at p. 443. http://www.uncitral.org/pdf/english/yearbooks/yb-1991-e/yb_1991_e.pdf (obtained on 12/12/2005).
[32] ibid.
[33] Ernest T Patrikis, Thomas C Baxter Jr. and Raj K Bhala, *Wire Transfers: A Guide to U.S. and International Laws Governing Funds Transfers*, Irwin, Illinois, 1993 at p.273.
[34] ibid.
[35] ibid.
[36]Bergsten 1996, note 17 supra at p. 443.

handwritten signature. [37] This means that where the originator's signature is forged, the originator's bank is not entitled to debit the customer's account, because the bank does not have the authority to do so.

Conversely, under Article 5 (2) of the UNCITRAL Model Law, the customer is bound by an authenticated payment order, whether it is in fact authorised or not, when the payment order is authenticated by means which are not "a mere comparison of signature." [38] Article 5(2) provides

> " (2) [W]hen a payment order or an amendment or revocation of a payment order is subject to authentication other than by means of a mere comparison of signature, a purported sender who is not bound under paragraph (1) is nevertheless bound if
> (a) the authentication is in the circumstances a commercially reasonable method of security against payment order, and
> (b) the receiving bank complied with the authentication."

Article 5(2) sets out two conditions that should be met to make the customer bound by authenticated payment orders, irrespective of whether the payment order is in fact authorised or not. First, the authentication system (security procedures) implemented by the originator's bank to authenticate the payment order should be "commercially reasonable." Second, the originator's bank must comply with the authentication system. [39] The originator's bank should meet the above-mentioned conditions; otherwise the bank is not entitled to debit the originator's account. When the bank does not meet both conditions, the bank bears the risk for unauthorised payment orders. [40] Further, under UNCITRAL Model Law, parties are forbidden to agree that

---

[37] ibid.
[38] Bergsten 1996, note 17 supra at p.444.
[39] The Uncitral Model Law on International credit Transfer 1992, Article 5 (2)(b) and ibid, at p. 444.
[40] Patrikis, Baxter and Bhala 1993, note 33 supra at p.274.

the customer might be bound by unauthorised payment order if the authentication is not commercially reasonable.[41]

Thevenoz has demonstrated that allocating the liability for authenticated but unauthorised payment order to the originator under the UNCITRAL Model Law is justifiable, as follows. In EFT the issuance, the amendments and the revocation of the payment order is conducted by using electronic means, it is hard to keep the natural relationship between the payment order and the "natural person who issues it." [42] Thevenoz continued that the person who possesses the terminal or the machine from where the payment order is sent is the best person to protect and prevent unauthorised use of the machine. [43] Therefore, the originator who possesses the machine or the computer in his premises should secure it from unauthorised access. However, the UNCITRAL Model limits the originator's liability for authentication, but an unauthorised payment order by stipulating that a "commercially reasonable" authentication system should be implemented and complied with.

Nevertheless, authenticated but unauthorised payment orders could be executed not only because of the customer fault or through accessing the machine that exists on his premises. Also, authenticated and unauthorised payment order could be executed by a hacker who managed to intercept the originator and the originator's bank communications. The hackers attack the security procedures and obtain unauthorised

[41] The Uncitral Model Law on International Credit Transfer 1992, Article 5 (3).
[42] Thevenoz, note 4 supra at p. 937.
[43] ibid.

access to the originator's account by different methods such as "sniffers," "Trojan Horses" and "Hijacking." [44]

In this sense, it should be emphasised that under the UNCITRAL Model Law the originator might shift back the liability for authenticated but unauthorised payment orders to the bank, where the customer can prove that an unauthorised payment order was not sent by a person, either a former or present employee of the customer or "a person whose relationship with customer enabled him to gain access to the authentication procedures." [45] However, the bank can shift back the liability to the originator, when the bank proves that the person who sent unauthorised payment order gained access to the authentication procedures through the fault of the customer.[46] The former cases of shifting liability between the parties under Article 5(4) of the UNCITRAL Model Law will not be examined in this chapter, to avoid repetition, and will be examined in Chapter five.

The present author's view is the policy of the UNCITRAL Model Law under Article 5, in terms of the allocation of risk makes the originator and the originator's bank more certain about their liabilities for authenticated payment order. Further, the allocation of risk for authenticated payment order on the customer forces the bank to implement a "commercially reasonable" authentication system and to comply with an authentication system. Furthermore, imposing such a duty on the originator's bank protects the originator from some type of unfair terms in the originator's bank contract. Where the originator's bank does not have a "commercially reasonable"

---

[44] Internet Banking: Comptroller's Handbook, Comptroller of the currency Administrator of national banks, (hereafter Internet Banking Comptroller's Handbook) October 1999 at p.71. See Chapter one Section 1.2.4.(a) for more details.
http://www.occ.treas.gov/handbook/intbank.pdf
http://www.occ.treas.gov (obtained 25/4/2004).
[45] The Uncitral Model Law on International Credit Transfer 1992, Article 5 (4).
[46] ibid.

authentication system, and includes terms in the contract to exclude and limit the bank's liability for an authenticated but unauthorised payment order executed by a third party. Article 5 (3) the UNCITRAL Model Law stipulates that parties are not allowed to agree on security procedures which are not commercially reasonable. This is because the allocation of parties' liabilities, in the case of an unauthorised payment order depends heavily on the security procedures implemented to authenticate the payment order. Article 5 (3) limits and restricts the originator's bank's use of its economic power to stipulate terms in the contract makes the originator bears the liability for authenticated but unauthorised payment order were not authenticated by "commercially reasonable" authentication system. [47] The next section of this chapter demonstrates which security procedures are considered as "commercially reasonable" security procedures under the UNCITRAL Model Law.

Article 5 (2) of the UNCITRAL Model Law improves the originator's bank's ability to execute payment orders at high speed and low cost, as the originator's bank liability for authenticated but unauthorised payment are predictable and certain. Thevenoz rightly argues that policies behind apportioning the risk of authenticated payment order under Article 5(2) are to ensure certainty and efficiency in business transactions.[48] He further argues:

> "[S]ince speed and low cost are principal advantages of electronic funds transfers, bank must be able to reach a quick and reliable decision regarding whether to execute any single payment order. The decision should be final if it supported by a "commercially reasonable" security procedure. Secondly, the provision [Article 5 of the UNCITRAL Model Law] [49] assumes as a matter of fact that, so long as banks comply with such procedures, their clients are in the best position to avoid fraud, and it is much less expensive for clients to take additional precautions." [50]

[47] Commission Report 1991, note 26 supra at p.18, para 111.
[48]Thevenoz, note 4 supra at p. 937-938.
[49] Words in square brackets added.
[50] Thevenoz, note 4 supra at p. 937-938.

The bank in EFT is seeking to exclude or limit its liability for an authenticated but unauthorised payment order. Malaguti has explained that Article 5 of the UNCITRAL Model Law encourages the bank to implement "commercially reasonable" authentication system, because in this way, the bank will escape liability for an authenticated but unauthorised payment order. [51] The present author agrees that the former provision encourages the bank, but at the same time, the customer will feel secure and ensure that "commercially reasonable" authentication is implemented to protect his account from unauthorised access. Therefore, Article 5(2) provides benefits for the originator and the originator's bank at the same time.

In conclusion, the above examination of Article 5 of the UNCITRAL Model law illustrates that EFT needs to be regulated by particular rules, and should not be left to be governed by the rules of agency law or contract law. Such rules should take into consideration the rules of the UNCITRAL Model Law. In particular, the distinguishing methods used to authenticate electronic payment order and the effects of these methods on the parties' liabilities and the ability to execute EFT at high-speed and low cost.

[51] Maria Chiara Malaguti, *The Payment System in the European Union Law and Practice*, Sweet& Maxwell, London, 1997 at p. 203.

### 3.2.3 Authentication System under the UNCITRAL Model Law.

Article 5 of the Model Law does not in itself lay down the guidelines, standards and factors that could be relied upon to determine whether the authentication system (security procedures) is commercially reasonable. [52] The Study Group of the UNCITRAL Model Law did not set out such guidelines or standards, and justified this by saying that what is "commercially reasonable" might be changed over time with the evolution of technology. [53] Further, the commercial reasonableness of the authentication system varies according to the circumstances of each fund transfer. [54] Hence the Study Group decided to add the following words "in the circumstance" before "commercially reasonable," pointing out that what is "commercially reasonable" depends on the circumstances of every funds transfer transaction. [55] However, Patrikis *et al* have argued that in the absence of such guidelines or standards, there is a possibility of inconsistency between judgements in respect of what is deemed to be a "commercially reasonable" authentication system.[56] The present author does not agree with Patrikis *et al* because the word "circumstances," which comes before "commercially reasonable", can be considered as guidelines for the court. The official report that was prepared by the Secretary-General of UNCITRAL on the Model Law provides examples of the factors that the court should take into consideration to determine whether the authentication system is "commercially reasonable." [57] These examples include the nature of the payment order, whether electronic or paper-based, the amount of the payment order and the

[52] Report of the Secretary-General 991, note 31 supra at p. 65, para 9.
[53] ibid.
[54] ibid.
[55] Commission Report 1991, note 26 supra at p.17-18 paras 106-113.
[56] Patrikis, Baxter and Bhala 1993, note 33 supra at p.274.
[57] Report of the Secretary-General 991, note 31 supra at p. 65, para 9.

parties' agreement on the procedures should be implemented and followed. In particular when the originator chooses less secure authentication system after the bank offered him more secured systems.[58] As Bergsten confirms:

> " [T]he Model Law does not attempt to delineate what would be a commercially reasonable method of security against unauthorised payment orders... .While something less than state-of-the-art technology or methodology would still be commercially reasonable, what is commercially reasonable in a given circumstance could be expected to change over time as new authentication technique becomes available. Moreover, even though the risk loss cannot be shifted to the sender by agreement with the bank when authentication procedure provided by the bank is not commercially reasonable, a choice by the sender to use less secure authentication procedure than another offered by the bank that was clearly commercially reasonable for that customer may be of significance in deciding whether the procedure used was commercially reasonable." [59]

The present author does not agree that the absence of guidelines may cause inconsistency in the court decisions, because each funds transfer transaction has different circumstances.

While the Study Group was working on the UNCITRAL Model Law there was parallel work and preparations in US for a law governing wholesale funds transfer. [60] In 1989, the National Conference of Commissioners on Uniform States Laws (NCCUSL) and the American law Institute (ALI) adopted Article 4A funds transfer. [61] Article 4A was added to the Uniform Commercial Code (UCC) and submitted to the legislatures of the different states, to be adopted in every State. [62] This is because the UNCITRAL Model Law and Article 4A regulates wholesale funds transfer and they

---

[58] ibid.
[59] Bergsten 1996, note 17 supra at p. 444.
[60] ibid at p. 414 and Thevenoz, note 4 supra at p.882-893.
[61] Bergsten 1996, ibid at p. 415, Thevenoz, ibid at p 882 and Benjamin Geva, The Law of Electronic Funds Transfers; Global and Domestic Wire Transfers, ACH payments, Consumer Transactions, Mathew Bender, New York, 1994 at p.1-35.
[62] ibid and Article 4A of the Uniform Commercial Law 1989.
http://www.law.cornell.edu/ucc/4A/ (obtained 08/02/07)
http://www.ali.org/

almost similar. [63] Moreover, Article 4A has influenced the UNCITRAL Model Law, because the work on Article 4A was always ahead of the work on the UNCITRAL Model. [64] The next section of this chapter is an examination and assessment for Article 4A as an example or a case study of adopting the minimum standards of UNCITRAL Model Law rules. The next section of this chapter in addition to the subsequent chapters of this thesis, will demonstrate that under Article 4A, the originator and the originator's bank rights, duties and liabilities for fraudulent EFT are more predictable and certain.

[63] Thevenoz, ibid at p.882-893, Bergsten 1996, ibid at p. 415 –417 and Benjamin Geva, *Bank Collections and Payment Transactions, Comparative Study of Legal Aspects*, Oxford [UK] New York: Oxford University Press, 2001at p.210.
[64] ibid.

## 3.3. ARTICLE 4A OF THE UNIFORM COMMERCIAL CODE (UCC) AND UNAUTHORISED EFT.

### 3.3.1 Article 4A of the UCC

In the US, modern computer and communication technology have increased the daily amounts of international wholesale EFT, as they are conducted quicker, at lower cost and are more efficient than paper-based funds transfer. [65] Before Article 4A was introduced the relationship between the bank and its customer was governed by case law and by analogy with the general principals applicable to other areas of law such as agency law and contract law. [66] Such sources were inadequate, and incapable of dealing with the problems arise in the context of fraudulent EFT. [67] In regards to case law, Patrikis *et al* state that

> "[E]xisting case law, instead of clarifying the issues, added to the confusion. Judge-made law tends to be uncertain, inconsistent and, by its nature, *ad hoc*. Rapidly changing technology and financial practices have so outstripped established precedents that case-by-case adjudication is ill-equipped to deal with issues raised by high speed, high volume, electronic funds transfers. This resulted in the unsavoury position of the parties to a funds transfer operating in legally uncertain terrain while awaiting an unpredictable judicial resolution."[68]

Ernest *et al,* Baker and Brandel rightly confirmed that depending on the case law leads the parties to further confusion and uncertainty about their rights and obligation towards each other, different judges established different rules. [69] Equally important is the fact that the contract cannot alleviate the uncertainty of the bank customer's

---

[65] Carl Felsenfeld, " Article 4A of the United States Uniform Commercial Code," Walther Hadding, and Uwe H. Schneider (eds), *Legal Issues in International Credit Transfers*, Duncker & Humblot, Berlin 1993 at p. 346-347.
[66] Ernest T. Patrikis, Raj K. Bhala and Micheal T. Fois, "An Overview of United States Funds Transfer Law," Robert C. Effros (ed), *Payment Systems of the World*, Oceana Publications, New York, London, 1996 at p. at p. 5-6.
[67] ibid.
[68] ibid.
[69] ibid and Donald I. Baker and Roland E. Brandel, *The Law of Electronic Fund Transfer Systems: Legal and Strategic Planning,* revised edition, Warren, Gorham & Lamont, Boston, 1996, at p. 13-3 – 13-4.

rights and obligations, due to the fact that different parties reach different agreements. This does not help to establish the uniformity of aiding the funds transfers as a whole.[70] Moreover, the inequality in bargaining power between the bank and the customer makes the contract approach incapable of offering a reliable solution. [71]

Legal uncertainty and economic inefficiency have emerged as a result of gaps in the different laws governing EFT, as such laws were focused on the bank to bank relationship, not the bank-customer relationship. [72] The gaps, legal uncertainty and economic inefficiency have increased the economic cost for EFT. [73] The former problems were the major factors behind adopting Article 4A. [74] As the Official Comment of Article 4A demonstrates:

> "[T]he funds transfer governed by Article 4A is in large part a product of recent and developing technological changes. Before this Article was drafted there was no comprehensive body of law--statutory or judicial--that defined the juridical nature of a funds transfer or the rights and obligations flowing from payment orders. Judicial authority with respect to funds transfers is sparse, undeveloped and not uniform. Judges have had to resolve disputes by referring to general principles of common law or equity, or they have sought guidance in statutes such as Article 4 which are applicable to other payment methods. But attempts to define rights and obligations in funds transfers by general principles or by analogy to rights and obligations in negotiable instrument law or the law of check collection have not been satisfactory." [75]

Article 4A of UCC regulates the funds transfer transactions from the point at which the originator instructs his bank to credit the beneficiary's account until the point the beneficiary's account is being credited. Harrell confirms as follows:

---

[70] Patrikis, Bhala and Fois 1996, ibid at p. 6 and Baker and Brandel, ibid at p.13-4.
[71] ibid.
[72] Patrikis, Bhala and Fois 1996, ibid at p.6.
[73] ibid.
[74] ibid.
[75] The official Comment on Article 4A issued by The American Law Institute (ALI) and The National Conference of Commissioners on Uniform State Law (NCCUSL), 1989, (1) of U.C.C 4A-S.102. (Hereafter the Official Comment).

> " [A]rticle 4A provides an efficient, comprehensive set of rules to govern funds-transfer that can total billions of dollars over short period time. Prior to Article 4A, there was no orderly body of law governing such transactions, and participants in this modern and efficient system of funds-transfers were subject to considerable legal risk and uncertainty.
> Article 4A preserves the principle of party autonomy, allowing the parties to a funds-transfer to create a legal environment suitable to their needs. It also provides clear-cut choice of law rules suitable to multi-jurisdictional funds-transfers. It creates a uniform legal foundation for funds-transfers, and provides specific rules governing common issues that are unique to such transactions."[76]

Article 4A permits variation by agreement with substantive provisions of its sections. Such variations are effective between parties agreeing to them.[77] The parties can vary the provisions of article 4A by agreement pursuant to section 501(a). Section 501 (a) of Article 4A states that "except as otherwise provided in this article, the rights and obligations of a party to a funds transfer may be varied by agreement of the affected party."

Patrikis *et al* confirm that Article 4A " promotes legal certainty and economic efficiency in funds transfers." [78] Article 4A a comprehensive law governs the parties rights, obligation and liabilities for EFT. [79] Article 4A has set out the solution for the most significant problems in EFT, which are the authenticity of the payment order and unauthorised payment order. [80] Furthermore, Article 4A allocates the risk between the parties, in the case of fraud, and imposes on the originator's bank duty to

---

[76] Alvin C. Harrell, "Wholesale Funds Transfers-UCC ARTICLE 4A," Chris Reed, Ian Walden, and Laura Edgar, (eds), *Cross-Border Electronic Banking, Challenges and Opportunities*, 2nd ed, Published Jointly with The Centre For Commercial Law studies, Lloyd's of London Press, 2000 at p.57.
[77] Geva 1994, note 61 supra at p. 1-37.
[78] Patrikis, Bhala and Fois 1996, note 66 supra at p.6.
[79] ibid and Baker and Brandel, note 69 supra at p. 13-5.
[80] Patrikis, Bhala and Fois 1996, ibid at p.21.

implement commercially reasonable security procedures. [81] These issues will be discussed in detail in subsequent chapters.

### 3.3.2 Unauthorised EFT in Article 4A of UCC

In the US, Article 4A as well as the UNCITRAL Model Law devotes particular rules that apply to the payment orders authenticated by using electronic means which are different from the rules apply to paper-based payment order. [82] The Official Comment of Article 4A explained that the rules of agency law in the context of EFT "give the receiving bank very little protection" and these rules only work well in the context of paper-based payment order. [83] Since EFT involves large amounts of money transferred at high speed and low cost, the receiving bank will be reluctant to accept the payment order unless it is ensured that the payment order is authorised. The assurance in EFT is obtained by depending on security procedures which are incomparable to a hand written signature. [84] The Official Comment of Article 4A states:

> "[I]n the wire transfer business the concept of "authorisation" is different from that found in agency law. In that business a payment order is treated as the order of the person in whose name it is issued properly tested pursuant to a security procedure and the order passes the test.
> Section 4A-202 reflects the reality of the wire transfer business. A person in whose name a payment order is issued is considered to be the sender of the order if the order "authorised" as stated in subsection (a) or if the order is "verified" pursuant to a security procedures in compliance with subsection (b). If subsection (b) does not apply, the question of whether the customer is responsible for the order is determined by the law of agency." [85]

[81] ibid at p.22-23.
[82] Article 4A Section 202 (a) & (b).
[83] The Official Comment, note 75 supra, Comment (1) on Section 4A -203.
[84] ibid.
[85] ibid.

Patrikis *et al* argue that Article 4A has developed a new solution which makes banks more confident and secure about accepting payment orders and executing them at high-speed. Article 4A has developed rules that specifically address the validity of security procedures, and which substitute a written signature with security procedures to detect unauthorised electronic payment orders. [86]

As a result of the distinctive nature of EFT authentication procedures, Article 4A sets out rules which allocate the liability between the customer and the bank for unauthorised payment orders.[87] If the bank executes a payment order in good faith, depending on a payment order that has been tested by the security procedures - agreed upon- and commercially reasonable, then the customer is obliged to pay the amount of money to the bank, whether the order is in fact authorised or not. [88] Pursuant to s.202 (b) of Article 4A:

> "[I]f a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorised, if (i) the security procedure is a commercially reasonable method of providing security against unauthorised payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security producer and any written agreement or instruction of the customer restricting acceptance of money payment orders issued in the name of the customer."

Patrikis *et al* aptly explain that the effect of s.202 (b) is to allocate the risk of loss on the customer for an unauthorised payment order, provided that the bank accepts the payment order after verifying it with "commercially reasonable" security

[86] Patrikis, Bhala and Fois 1996, note 66 supra at p.22.
[87] ibid.
[88] Baker and Brandel, note 69 supra at p. 13-32 and Patrikis, Bhala and Fois 1996, ibid.

procedures.[89] According to s.202 (e), s.202 "applies to amendments and the cancellation of payment orders to the same extent it applies to payment orders."

The present author argues that under section 202 (b) the originator and the originator's bank rights, duties and liability for authenticated but unauthorised payment order are more predictable and certain than under common law. This is because section 202 (b) proportions the liability between the parties by stipulating that specific requirements should be met to allocate the liability. Thevenoz confirms that the implementation of "commercially reasonable" security procedures is the "cornerstone" to determine the originator and the originator's bank liability for authenticated but unauthorised payment orders. [90] The originator's bank is obliged to implement commercially reasonable security procedures, agreed on with the originator, so as to verify the payment orders send by the originator. If the payment order is verified by commercially reasonable security procedures, the payment order is deemed to be an authorised payment order, even though in fact it is not. Accordingly, the bank could be certain in advance that is entitled to debit the customer's account on the basis of the authenticated payment order irrespective in fact it is unauthorised. Consequently, the bank would not be reluctant to execute the payment order at high speed and low cost, because the bank's liability is predictable and certain. Furthermore, imposing a duty on the bank to implement "commercially reasonable" security procedures protects the originator from unfair contract terms that the originator's bank includes in the bank account agreement. Such terms are drafted to exclude or limit the banks' liability for authenticated but unauthorised payment orders, irrespective of whether the implemented security procedures are "commercially reasonable" or not.

---

[89] Patrikis, Bhala and Fois 1996, note 66 supra at p.23.
[90] Thevenoz, note 4 supra at p.936.

Further, under section 202 (b), in addition to the bank duty to implement commercially security procedures, this section imposes on the originator's bank other duties to avoid liability for authenticated but unauthorised payment order. The originator's bank must approve that it accepts the payment order in good faith and in compliance with the security procedures. [91] The bank is under a duty to train its employees to "test" the payment orders, in compliance with security procedures and steps, and the bank will be responsible for those of its employee's acts which do not comply with the security procedures.[92] The bank is liable if an unauthorised payment order is not detected as a result of the bank's non-performance of the required security procedures. [93]

Article 4A defines "good faith" as honesty in fact and in the observance of reasonable commercial standards of fair dealing."[94] The definition of good faith, according to Article 4A, requires two factors to satisfy: honesty and reasonable commercial standards. These requirements mean that the bank should execute the payment order honestly and with "reasonable behaviour." [95] Patrikis *et al* state as follows: "if a party acts recklessly and maliciously, but is honest, then (arguably) that party has not acted in "good faith" under Article 4A definition because it has not acted reasonably."[96]

The bank must prove that it complied with any agreement and instruction that restricts the acceptance of payment orders pursuant to s.202 (b) (ii) of Article 4A. Where the

---

[91] Baker and Brandel, note 69 supra at p. 13-33
[92] The Official Comment, note 75 supra, Comment (3) on Section 4A -203.
[93] ibid.
[94] U.C.C s. 4A-105 (a) (6).
[95] Patrikis, Baxter and Bhala 1993, note 33 supra at p.43.
[96] ibid.

customer imposes instructions of the payment orders that the bank must accept, the bank must not accept any payment order against these instructions. For example, the customer may forbid the bank to accept a payment order that exceeds a specific limit, or may prohibit the bank from accepting more than a limited numbers per week or days. If the bank does not follow the customer's instructions and accepts a payment order against his instruction, pursuant to s.202 (b) (i), such a payment order is an unauthorised payment order, and the bank cannot debit the customer's account.

In *Tomaz Mendes Regatos* v *North Fork Bank and New Commercial Bank of New York,* [97] the plaintiff opened a bank account with New Commercial Bank of New York (CBNY) the defendant. The parties agreed that Regatos could make wire transfers from his home in Brazil by signing a payment order form and then fax the form to the CBNY representative office in Sao Paulo, Brazil. After sending the fax the plaintiff would call the CBNY representative to confirm that payment order form was received. If Regatos did not call the representative, he would call him to confirm the payment order. According to the confirmation, the CBNY representative would send the form by fax to the bank in New York, where the employee there would check the signature on the faxed form against Regatos' signature card, which the Bank kept on file. In 2001, the CBNY debited Regatos' account on two different occasions, depending on two different payment orders that were allegedly sent by Regatos. Regatos contended that he neither sent, nor authorised both payment orders. In this case, the appellant could not confirm that a confirmation had been obtained from Regatos after the payment order form had been received by the CBNY representative. Accordingly, the Second Circuit Court of Appeal held that:

---

[97] Tomaz *Mendes Regatos v North Fork Bank and New Commercial Bank of New York* 396 F. 3d 493 (Court of Appeals 2nd Cir January 2005).

> "[T]he "effectiveness" of a payment order is defined by section 4-A-202, which provides that "a payment order ... is effective ... if (a) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, *and* (b) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure ...." The jury in this case found that CBNY had failed to prove that it had executed the transfers "in compliance with the security procedure.".[98]

Consequently, in EFT, the payment order is an authorised payment order and the bank can debit the customer's account if the following conditions are met together in the payment order: first, agreement on the security procedures; second, compliance with security procedures; third, the bank must act in good faith; fourth, compliance with customer instructions; and lastly, compliance with commercial reasonableness of security procedures, which will be discussed in the next section. Hence, the former conditions must be met together to apply subsection (b). If one of these conditions do not exist subsection (b) does not apply, and this in turn means that subsection (a) as a general rule applies. Thus, the bank will bear the risk if the payment order is an unauthorised payment order, as the bank in such a case cannot debit the customer's account. [99] Subsequently, such a payment order is not binding on the customer and the customer can ask the bank to credit his account with that amount of money, as it was debited according to an unauthorised payment order.

In *Hedged Investment Partners, L.P.* v *Norwest Bank Minnesota,* [100] Hedged Investment Partner (HIP) signed an agency agreement with Norwest Bank authorising the bank to conduct certain wire transfer services on their behalf. The agency agreement stipulated *inter alia* that HIP provided Norwest bank with signatures to be

---

[98] ibid, at p. 495-496.
[99] The Official Comment, note 75 supra, Comment (3) on Section 4A -203.
[100] *Hedged Investment Partners, L.P., et a.l* v *Norwest Bank Minnesota, N.A.* 578 N.W.2d 756(Minn. App 1998).

used to verify HIP communication with Norwest bank. HIP sued Norwest bank for 19 wire transfer totalling $499,000, alleging *inter alia* that none of these 19 wire transfer were authorised properly according to the agency agreement. The Court of Appeal of Minnesota held that it was Norwest bank's duty to check the signature on the written payment order according to agency agreements, and did not establish a "commercially reasonable" security procedures under Article 4A. [101] As Section 201 of Article 4A states:

> "[A] security procedures may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure."

Given that a mere comparison of signature is not a security procedure under Article 4A the Court of Appeals held that Section 202(b) did not apply in determining whether the payment order was authorised or not. Hence the court concluded that Section 202 (a) must be applied, to determine whether the payment order was authorised or not, according to the rules of agency law. The Court of Appeal stated as follows

> "[T]he responsibilities Norwest assumed that are covered under Article 4A fit squarely within the concept of "authorization" under Minn.Stat. Section 346.4A-202(a). The payment orders in question were transmitted in writing from a known source with whom the bank had personal contact. By agreeing to check the signatures of the limited partners and check the wire instructions provided by new investment advisors, Norwest agreed to determine whether the payment orders were authorized. These responsibilities did not establish a commercially reasonable method of determining whether the payment orders were authentic." [102]

Section 202 (a) of Article 4A stated:

---

[101] ibid, at p.774
[102] ibid.

> "[A] payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under agency law."

Section 202(a) of Article 4A set out a general rule to determine whether the payments order an authorised payment order or not. This subsection (a) stipulates that in the absence of any statute or agreement that specially regulates such payment orders, the law of agency is applied to determine whether the payment order authorised or not. [103] Consequently, in such cases, the actual authority, apparent authority and authority by estoppel are applicable, [104] similar to the situation under the common law in UK.

Under Section 202 (a) the receiving bank accepts the payment order, which is authorised by the person who is identified to be the sender of the payment order according to the bank-customer agreement. The authorisation could be specific or general, for one transaction or more. [105] Geva explains that if the receiving bank executed a funds transfer depending on a payment order which was authorised by a person identified as the sender, the bank can debit the customer account with that amount of money and credit the beneficiary's account or the next party in the chain. Thus, the customer is obliged by the authorised instructions sent by an authorised person. [106] In a paper-based payment order, the bank can identify whether the person who sends the payment order is authorised to do so by verifying his signature, whereas in EFT, the bank cannot identify who is the person transmitting the payment order and whether he is authorised to do so or not. [107] This is because the bank receives the payment order by electronic means that lack face-to-face connection.

---

[103] The Official Comment, note 75 supra, Comment (3) on Section 4A -203 and Thevenoz, note 4 supra at p. 935.
[104] ibid.
[105] Geva 1994, note 61supra at p.2-66.
[106] ibid.
[107] The Official Comment, note 75 supra, Comment (1) on Section 4A -203.

This makes the bank reluctant to accept payment order unless it has the assertion that the payment order is what it purports to be. [108] This is why Thevenoz argues that applying agency law to determine whether authorised payment order or no does not give the bank and its customer adequate protection in relation to unauthorised payment order in the context of EFT. [109] Therefore, Article 4A adopted Section 202(b) to solve the problem of identity authentication and its effects on the originator and the originator's bank liability for authenticated but unauthorised payment order. Felsenfeld states that the bank will not have the time or the required information to obtain such an assertion, as EFT transactions are transmitted by using high-speed electronic means. [110] He continues under Section 202 (b) and relying on the security procedures the bank is able to determine quickly whether the payment order is authorised or not and retransmit it to the next bank in the chain. [111]

### 3.3.3 Legal Concept of Security procedures in the context of EFT under Article 4A of U.C.C.

In the US, security procedures are recognised in statutory rules, as well as the required standard of the security procedures that must be implemented. [112] Section 201 of Article 4A defines "security procedure" as follows:

> "..a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure."

---

[108] ibid.
[109] Thevenoz, note 4 supra at p. 935- 938.
[110] Felsenfeld, note 65 supra at p.351.
[111] ibid.
[112] See the Uniform Commercial Code 1992, Article 4A s.201 and 202 (c)

The definition sets out that the security procedures must be established according to the customer's and receiving bank's agreement. This definition does not apply to the security procedures the bank uses unilaterally. [113] Moreover, the definition stipulates two functions for security procedures. First, to confirm that the payment orders or the amendments or the revocation have been issued by the customer and second, to detect the error in the message information or the multiple transmission of the payment order. [114]

The definition does not consider a mere comparison of a specimen signature of the customer, a security procedure in itself. As mentioned in the previous section of this chapter, the Court of Appeal held that the bank's duty to check written signature is not a security procedure, pursuant to Section 202 of Article 4A. [115] The term provides examples of what might be deemed security procedures, for example algorithms or other codes, identifying words or numbers, encryption and callback procedures. Felsenfeld has stated that "the definition is deliberately broad in scope and less than specific in order to accommodate whatever sort of technical development may be found appropriate." [116] The definition is sufficiently broad to recognize new forms of signature that may arise as result of information technology developments.

The effect of s.202 (b) of Article 4A is to place the risk of loss on the customer for an authenticated payment order, as verified by the bank, in compliance with a commercially reasonable security procedure. The bank cannot benefit from subsection (b) unless it has made available to the customer security procedures that are

[113] Baker and Brandel, note 69 supra at p.13-34.
[114] The Official Comment, note 75 supra, Comment on Section 4A -201
[115] *Hedged Investment Partners,* note 101 supra at p.774.
[116] Felsenfeld, note 65 supra at p.351.

commercially reasonable. Thus, both parties in advance can predict their rights, duties and liabilities for an authenticated payment order, irrespective it authorised or not. Under Section 202(b) of Article 4A an authenticated payment order is authorised, whether it is in fact authorised or not. This certainty is not available under agency common law, as under agency law authenticated payment orders might be authorised or not. Depending on whether the payment order is in fact authorised or not and according to different doctrines of agency law the actual authority, apparent authority and authority by estoppel are applicable.

Article 4A-202 (c) has stated that to determine the commercial reasonableness of security procedures is a question of law, taking into consideration variable factors, such as the customer's instructions expressed to the bank, the type, size and frequency of payment orders. The Official Comment to Article 4A provides as follows

> "[I]t is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers." [117]

Consequently, when the court examines whether security procedures are commercially reasonable, it should take into consideration the standard of security procedures that are mostly adopted within the banking industry. Furthermore, the court considers whether such security procedures that are in general used by the customers and the receiving bank in a similar situation. In the *Centre-Point Merchant Bank Ltd v American Express Bank Ltd* [118] case, the court has taken the former factors into consideration in its judgement. The plaintiff was a Nigerian banking institution that had entered into a banking relationship with American Express Bank

[117] The Official Comment, note 75 supra, Comment (4) on Section 4A -203.
[118] *Centre-Point Merchant Bank Ltd v American Express Bank Ltd*, 2000 WL 1772874 (S.D.N.Y).

(AEBL). For security reasons, parties who communicated almost exclusively by telex, agreed in March of 1989 to "test" all telexed financial transaction between them by using a telegraphic test key code. On 19 August, 1993 AEBL received two fraudulent payment orders, both of them tested properly pursuant to the test key security procedure. AEBL honoured them both. The plaintiff alleged *inter alia* that AEBL failed to provide a "commercially reasonable" security procedure by using a telegraphic test key code. Duffy J has stated that

> " [A]s even the plaintiff's expert admitted, in 1993 all the bank in Nigeria used the same security procedure: the telegraphic test key. Consequently, this was the procedure AEBL used with all of its Nigerian banks and the One Centre-Point used with all of correspondent banks with which it did business. For the reasons stated above, therefore, I find the security procedure that the parties in this case agreed to was "Commercially reasonable" one under Article 4A." [119]

Moreover, the methods used to transmit the payment order may affect the type of security procedures deemed to be commercially reasonable. [120] For instance, the security procedures used in Internet communications are different from the procedures used within a dedicated telecommunication infrastructure. [121] The Internet is an open network, and therefore, the security procedures used over the Internet are more sophisticated and complex than the security procedures used over a dedicated network (closed networks). [122]

Furthermore, to determine the commercial reasonableness of security procedures, the "customer wishes," the amount and the number of payment orders the customer may issue must be taken in consideration. [123] For instance, the customer who issues many payment orders in large amounts may be very keen to choose security procedures

---

[119] *Centre-Point Merchant Bank Ltd v American Express Bank Ltd* at p.5.
[120] The Official Comment, note 75 supra, Comment (4) on Section 4A -203.
[121] UNCTAD, *E-Commerce and Development Report 2002*, United Nations, New York 2002 at p.135.
[122] See Forms of Security Procedures in Chapter two.
[123] The Official Comment, note 75 supra, Comment (4) on Section 4A -203.

which are highly developed, regardless of the cost. On the other hand, the customer who occasionally issues payment orders in medium or small amounts, compared to the former customer, may insist on using a higher-risk security procedure because it is cheaper and more convenient. [124] In *Centre-Point Merchant Bank* Duffy J has stated

> "[T]he official comment to Article 4-A-203 provides some guidance for the court in determining the reasonableness of a bank's security procedures:
> A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedures is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower a standard...In most cases, the mutual interest of bank and customer to protect against fraud should lead to agreement to a security procedure which is commercially reasonable.
> Moreover as provided in s 4A-203(3): Commercially reasonableness of a security procedures is ....to be determine by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank including the size, type, and frequency of payment orders normally issued by the customer to the bank...and security procedures in general use by customers and receiving banks similarly situated.
> As I apply these factors to the agreed-upon procedure at issue here, I find that the telegraphic test key meets the "commercially reasonable" standard required by the statute and that Defendant complied with such procedures. Furthermore, I find that, contrary to Centre-Point's allegations, the agreed-upon procedure including nothing more than what the telegraphic test key provided." [125]

Where the customer expressly refuses commercially reasonable security procedures that are offered by the bank, and insists on using a higher- risk security procedures, because they are cheaper, under Section 202 (c) of article 4A, such security procedures are deemed to be commercially reasonable, provided that the customer signs an agreement stating expressly that he is obliged to make any payment order the bank will accept according to the security procedures he has chosen and whether the payment order was authorised or not. [126] Section.202 (c) states that:

---

[124] ibid.
[125] *Centre-Point Merchant Bank Ltd v American Express Bank Ltd* at p.4-5.
[126] ibid and U.C.C section. 4A-202 (c) I & II

> "[A] security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security chosen by the customer."

In this case, the customer is liable for an unauthorised but properly authenticated payment order, even if the customer chooses security procedures which do not meet commercially reasonable standards. [127] The present author's view is that the purpose of this section is to give a clear explanation of what are deemed to be commercially reasonable security procedures, in order to protect the bank and the customer. This section is to determine the bank's and the customer's rights and obligations in respect of the security procedures used in their communications, which makes the liability for unauthorised EFT more predictable and ascertained.

In conclusion, Section 202 (c) of Article 4A provides the court with the following factors to determine the commercial reasonableness of security procedures. First, the "customer wishes" expressed to the bank; second, the circumstances of the customer known to the bank, the size, type and frequency of payment orders normally issued by the customer; third, alternative security procedures offered to the customer; and lastly, the security procedures that are in general used by customers and receiving banks in similar situations.[128] Patrikis *at el* note as follows:

> "[H]owever, this list of factors cannot possibly guarantee consistent judgments. Reasonable judges could come to different conclusions in applying this framework to the same security procedure. And, as an intellectual matter the test strains the distinction between questions of law and fact. Is not each of the factors listed a matter of fact? To the extent that any factor is regarded as a question of fact, a judge is asked to perform the fact finding. Nonetheless, the test for commercial reasonability is not meant to cause problems, and it may

[127] The Official Comment, note 75 supra, Comment (4) on Section 4A -203.
[128] Baker and Brandel, note 69 supra at p.13-35 and Patrikis, Bhala and Fois 1996, note 66 supra at p. 23.

> be defended as a pragmatic device, which affords an originator procedure and its bank freedom of choice in selecting a security procedure. The Drafting Committee did not want to force all customers to choose the same level of security, and rightly so." [129]

The present author's view is that even if such factors may not lead to the same conclusion in different judgements, such factors still do stipulate the minimum predictable outcomes of courts' judgements. Furthermore, these factors protect the customer from a situation where the originator's bank stipulates contract terms to exclude or limit its liability for authenticated but unauthorised payment orders, where commercially unreasonable security procedures are used. According to Article 4A the originator's banks cannot exclude or limit their liability if the implemented security procedures are commercially unreasonable.

## 3.4.CONCLUSION

The UNCITRAL Model law and Article 4A are developed legal frameworks, as they recognise the distinct nature of EFT authentication in a world of high-speed and large-value EFT. [130] The bank is now capable, pursuant to Article 4A and the UNCITRAL Model Law, of relying on the "security procedures" agreed upon, to determine quickly and securely whether to act upon the payment order. [131] Moreover, these framework recognise the impact of implementing electronic security procedures to authenticate payment orders and the parties' rights and obligations towards each other. Felsenfed has stated that

> " [I]n relying on this procedures [security procedures], the receiving bank need not establish that the order is in fact the order of the sender. The payment order may in fact have been sent by a completely unauthorised interloper. The

[129] Patrikis, Baxter and Bhala 1993, note 33 supra at p.44.
[130] Felsenfeld, note 65 supra at p. 351.
[131] ibid.

> task of the receiving bank thus becomes simpler and less expensive. It must, in the original establishment of the security procedures, ensure that the procedures is commercially reasonable. But this must be done only once. It must then ensure that in its recipient of every payment order it has followed the requirements of the procedure that the parties have put in place." [132]

Under the UNCITRAL Model Law and Article 4A, the bank is obliged to implement commercially reasonable security procedures to authenticate the payment order. Hence, the originator is protected against terms which exclude or limit the originator's bank for authenticated but unauthorised payment orders, where security procedures are commercially unreasonable. Under the UNCITRAL Model Law and Article 4A the originator's and the originator's bank rights, duties and liabilities for authenticated payment order, whether authorised or not, are more predictable and certain. This is because both the UNCITRAL Model Law and Article 4A provide rules recognising the significance of security procedures to authenticate electronic payment orders. Furthermore, the rules impose a duty on the originator's bank to implement "commercially reasonable" security procedures and give guidelines of the factor can be used to evaluate whether the security procedures are commercially reasonable. These rules confined the originator and the originator's bank liability for authenticated but unauthorised payment orders. The present author's view is that the above-mentioned rules achieve two important aims: firstly, the protections for both parties. In terms of the originator, the rules protect him from unfair contract terms. In terms of the originator's bank, it is protected from liability for authenticated but unauthorised payment orders, where the bank implements "commercially reasonable" security procedures. Secondly, these rules make the originator and the originator's bank rights, duties and liabilities for authenticated but unauthorised payment order more predicable and certain.

---

[132] ibid.

This chapter has examined the approach of the UNCITRAL Model Law and Article 4A to unauthorised EFT's. In chapter four the analysis moves on to the issue of fraudulent EFT with reference to English and EU law. In chapter five, the treatment of that question by the UNCITRAL and Article 4A is reviewed.

# CHAPTER FOUR

# PARTIES' LIABILITIES FOR FRAUDULENT WHOLESALE ELECTRONIC FUNDS TRANSFER IN ENGLISH AND EU LAW

## 4.1. INTRODUCTION

Fraudulent payment orders are unauthorised electronic funds transfers: although not all unauthorised EFT's are fraudulent. They may, for example, be erroneous payment orders. [1] In fraudulent EFT, the person who issues the payment order is neither the originator nor the person who is authorised to issue such payment orders. [2] This person (the fraudster) could be one of the customer's employees, one of the bank's employees or a third party. [3] It is submitted that in England, the bank-customer relationship in the context of EFT payment order is a "mandate" relationship, governed by agency law or mandate law [4] and contract law. [5]

This chapter argues that applying the rules of agency law and contract law to the originator's bank and the originator's liability for fraudulent EFT against each other is not appropriate to deal with the peculiarity of fraudulent EFT payment orders. Applying such rules to electronic payment orders leads to the uncertainty and unpredictability of the bank-customer's liability for fraudulent payment order. This is because first, banks have adopted

---

[1] Anu Arora, *Electronic Banking and the Law* 3rded, IBC Business Publishing, UK, 1997 at p.117, for more details on definition of fraud see section 1.2.4 of chapter one.
[2] Arora 1997, ibid.
[3] Jonathan lass, "Fraud, Error and System Malfunction: A banker's Viewpoint," Royston Goode, *Electronic Banking: The Legal Implications,* Institute of Bankers, London, 1985 at p. 59-60.
[4] *Royal Products Ltd v Midland Bank Ltd,* [1981]2 Lloyd's Rep.194.
[5] *Foley v. Hill,* (1848) 2 H.L. Cas.28 used as an authority in the judgment in Re Spectrum Plus Ltd; National Westminster Bank plc v Spectrum Plus Ltd and others, House of Lords, [2005] UKHL 41 and *National Bank of Commerce v National Westminster Bank* [1990] 2 Lloyd's rep.514

different schemes for sharing liability for fraudulent EFT between them and their customers. For example, some banks have adopted exclusive conditions in their contracts to limit and exclude themselves from liability for fraudulent EFT; meanwhile, other banks have decided to bear the whole liability for fraudulent EFT. [6] Moreover, banks mostly in their standard terms contracts exclude liability for the negligence of their intermediary banks that are engaged in funds transfer. [7] Second, the parties' liability for fraudulent EFT depends on the originator's bank's "broad duty" [8] to exercise reasonable care and skill in carrying out the payment order. Depending on such "broad duty" has led to unpredictable and uncertain liability, which will be discussed later in this chapter.

Furthermore, this chapter evaluates the rules of Cross-Border Credit Transfer Regulations 1999 and the EU Directive 97/5/EC on Cross-Border Credit Transfer in the context of the originator and the originator's bank liability for unauthorised EFT. This chapter will demonstrate that the UK Regulations and the EU Directive are limited in application, and do not solve the problems of parties' liability for fraudulent wholesale EFT. Firstly, the UK Regulations and the EU Directive only apply to wholesale EFT up to 50,000 Euro and secondly, this legislation is not comprehensive, as it does not set out particular rules for authorized and unauthorized payment order or the parties' liability for such fraudulent transactions.

Given the unpredictability and the uncertainty of the parties' liability for fraudulent EFT under English law, and in the absence of particular rules devoted to govern and regulate the

---

[6] Ahmed Azzouni, "Internet banking and the Law: a critical examination of the Legal controls over Internet banking in the UK and their ability to frame, Regulate and secure banking on the net," J.I.B.L.R. 2003, 18(9), 351-362 at p.361.

[7] Richard Hooley and John Taylor, "Payment by Funds Transfer," Michael Q.C. Brindle and Raymond Cox (eds) 3rd ed, *Law of Bank Payments*, Sweet& Maxwell, London, 2004, p.125-127.

[8] Benjamin Geva, *Bank Collections and Payment Transactions, Comparative Study of Legal Aspects*, Oxford, New York: Oxford University Press, 2001, at p.397.

parties' liabilities for fraudulent wholesale EFT, this thesis argues that such transactions need to be regulated. Further, given the limited application and the inadequacy of the Cross-Border Credit Transfer Regulations 1999 and the EU Directive 97/5/EC on Cross-Border Credit Transfer, this thesis argues that the UK regulations and the EU Directive need to be amended. Such amendments should take into consideration the minimum standards of the rules of the UNCITRAL Model and Article 4A as they apply to the bank-customer's liability for fraudulent wholesale EFT. These rules will be examined in the next chapter. The next chapter will demonstrate that the rules of the UNCITRAL Model Law and Article 4A stipulate the strict liability of the originator's bank and the originator for fraudulent payment orders. Moreover, the next chapter will demonstrate that determining the originator and the originator's bank's liability for fraudulent payment order is more predictable and certain than under English common law, the UK Regulations and EU Directive.

Section 4.2 of this chapter sets out the basis of the originator's action against the originator's bank for fraudulent EFT. Section 4.3 examines the originator's bank's liability under English law and the problems of uncertainty and unpredictability in determining which party bears liability for fraudulent EFT. Section 4.4 demonstrates the type of damage recoverable by the originator in the context of fraudulent EFT. Section 4.5 examines the originator's bank and the originator's liability for fraudulent EFT under the Cross-border Credit Transfer Regulations 1999 in UK, alongside the EU Directive 97/5/EC on Cross-Border Credit Transfer. This section demonstrates that the UK regulation and the EU Directive are not comprehensive and sophisticated, as they do not deal with fraudulent EFT. Therefore, this chapter will conclude that the UK Regulations and the EU Directive

these should be amended to cover the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT.

## 4.2. THE BASIS OF THE ORIGINATOR'S ACTION AGAINST THE ORIGINATOR'S BANK FOR FRAUDLENT EFT

It is submitted [9] that both cheques and EFTs are mandates issued by the customer to his bank to debit his account with a sum of money. Moreover, the originator's bank or the paying bank as an agent to its customer is under a duty to adhere to its customer mandate, and to execute the customer's mandate with reasonable skill and care. [10] Accordingly, the bank is not entitled to debit the customer's account according to an unauthorised payment order, regardless of the method used to issue the payment order. [11] As mentioned before [12] an analogy is drawn with the Bill of Exchange Act 1882 to determine the originator's bank liability for fraudulent EFT. According to the Bill of Exchange Act the bank that pays a forged cheque is not entitled to debit the customer's account for the amount of the cheque.[13] Moreover, the cheque is inoperative, when it bears a forged drawer's signature or the cheque details altered fraudulently. In both cases the bank is unauthorised to debit the customer's account.[14] By analogy, in the context of EFT, if the payment order is initiated by an unauthorised person or altered by an unauthorised person, it is an unauthorised payment order and the originator's bank is not entitled to debit the

[9] Hooley and Taylor, note 7 supra at p.109 and Geva 2001, note 8 supra at p. 393-400.
[10] Hooley and Taylor, ibid and Geva 2001, ibid.
[11] Mark Hapgood QC, *Paget's law of banking* 12th ed, Butterworths, London 2002 at p. 336.
[12] See section 2.3 of Chapter two.
[13] Bill of Exchange Act 1882 section 24.
[14] ibid and Andrew Laidlaw and Graham Roberts, *Law Relating to Banking Services* 2nd ed, The Chartered Institute of Bankers, London, 1992 at p. 124-125 and Graham Roberts, *Law Relating to Financial Services* 5th ed, The Chartered Institute of Bakers, Canterbury, 2003 at p.99-102.

originator's account. Moreover, the originator is entitled to claim for recrediting his account with that amount of money.

The basis of the originator's action against the originator's bank for unauthorised payment order is "founded on simple contract," [15] as the relationship between the originator and the originator's bank is a contractual relationship. When the originator's bank debits the originator's account upon an unauthorised payment order, the originator's bank breaches its duty under the contract by transferring money without the customer's mandate. [16] In *National Bank of Commerce* v *National Westminster Bank* the defendant debited the plaintiff's account with eight amounts totalling £ 268,227.08, in respect of eight mail transfer orders (MTOs) purporting to have been signed by two authorised officers of the plaintiff. The plaintiff alleged, but the defendant did not admit, that none of those MTOs were in fact signed by two authorized officers of the plaintiff. The plaintiff accordingly alleged that each of the eight debits were ineffective. In terms of whether the customer's action was based on contract or tort, Webster J. stated that "the claim is clearly not an action in tort: it is founded only on contract or contractual indebtedness. It is, therefore, an action founded on simple contract." [17] According to this "simple contract" the customer can establish three claims against the bank. Webster J. stated that

> "(T)he points of claim, on their face, contain, apart from the declaration, two sets of claims founded on contract: first, a claim to be repaid the principal sum in respect of which the defendant is alleged to be indebted to the plaintiff following a demand to repay that sum, and a similar claim in respect of interest on that sum; and, secondly, a claim for damages for breach of the obligation, under the "agreement governing the account," to repay each of those two sums (principal sum and interest)." [18]

---

[15] *National Bank of Commerce v National Westminster Bank* [1990] 2 Lloyd's rep.514 at p.516.
[16] Geva 2001, note 8 supra at p.98.
[17] *National Bank of Commerce v National Westminster Bank*, note 15 supra at p.516.
[18] ibid.

By analogy, whenever the originator's account is debited as a result of an unauthorised EFT, the originator is entitled to take action against the bank as founded on breach of contract a result of the originator's bank's breach of its duty under either the creditor-debtor relationship or the agent- principal relationship. [19] Accordingly, the originator is entitled to claim for repayment of the principal sum and interest. Moreover, the originator may be entitled to claim for damages depending on the account agreement. [20] The type of damages the originator can claim for will be discussed in a subsequent section in this chapter.

## 4.3. A CRITIQUE OF THE APPLICALITY OF COMMON LAW RULES OF AGENCY LAW AND CONTRACT LAW TO FRAUDULENT EFT

In England, there is a consensus that the parties' liabilities in the context of unauthorised EFT are currently governed by the general principles of contract or agency law, [21] and by the drawing of an analogy to this law as applicable to forged cheques. [22] The type of fraudulent EFT and the party that executes the fraudulent payment order affects the originator's and the originator's bank's liability for fraudulent EFT against each other. Thus, the negligence and fault of the originator or the originator's bank may facilitate the execution of fraudulent payment order by their employees or third party. In such circumstances, the originator's bank or the originator may be stopped from challenging liability for fraudulent EFT. The forthcoming pages will examine the originator's bank's liability and the originator's liability for an unauthorised EFT, and examines whether

[19] See Chapter Two for more details about the Creditor-Debtor relationship and the Agent –Principal Relationship.
[20] *National Bank of Commerce v National Westminster Bank*, note 15 supra at p.516.
[21] Hooley and Taylor, note 7 supra at p.119, Hapgood, note 11 supra at p. 332-340, Geva 2001, not 8 supra at p.393 and E. Ellinger, Eva Lomnicka and Richard Hooley, *Modern Banking Law* 4th ed, Oxford University Press, New York, 2005 at p.549-556.
[22] Hooley and Taylor, ibid, Hapgood, ibid, Geva 2001, ibid and Ellinger, Lomnicka and Hooley, ibid.

applying the rules of forged cheque is adequate in dealing with unauthorised EFT. This section will conclude that applying such rules leads to uncertainty and unpredictability of parties' rights and obligations. Accordingly, the forthcoming section examines the originator's liability when his negligence facilitates fraudulent EFT, and the scope of the originator's bank's liability for fraudulent EFT as a result of its negligence.

.

**4.3.1 The Originator's Liability when its Negligence Facilitates Fraudulent EFT**

The bank and customer's duties to exercise reasonable care and skill have determined the loss allocation of forged cheques between parties in court decisions. [23] Thus, the role of the customer and the bank's negligence or fault in facilitating cheque forgery has determined their liability for loss. [24] The present author's view is that the way of performing the duty of reasonable care and skill in the context of forged cheques is different from the way of performing the same duty in the context of fraudulent EFT. With respect to forged cheques the customer is under a duty to exercise reasonable care and skill in drawing cheques in a manner not to facilitate forgery. [25] For example, in *Young* v *Grote* [26] the court held that the customer did not exercise reasonable skill and care in drawing and signing a blank cheque and gave the opportunity for a clerk to fill it out with fraudulent amount. [27] In EFT, the payment order is initiated and signed electronically. Thus, the customer's duty to exercise reasonable care and skill in initiating and signing the payment order takes a different form

---

[23] *Young v Grote*, (1827), 4 Bing. 253, *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd. and others* [1986] A.C.80 and *London Joint Stock Bank, Limited v Macmillan and Arthur*,[1918] A.C.777.
[24] ibid.
[25] J. Wadsly, and A.G. Penn, *The Law Relating to Domestic Banking* 2nded, Sweet& Maxwell, London, 2000, at p.241.
[26] *Young* v *Grote,* (1827), note 23 supra, applied by *London Joint Stock Bank, Limited v Macmillan and Arthur*,[1918] A.C.777 and *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd. and others* [1986].
[27] ibid.

from drawing a blank cheque or leaving a space for words or numbers to be added so as to alter the cheque amount.

Indeed, the originator's fault or negligence may facilitate or contribute to initiating an authenticated but unauthorised payment order takes on a different form in EFT. [28] Thus, an unauthorised person may gain access to the computer terminal and initiate an unauthorised payment order. [29] Geva rightly believes that the customer's negligence in initiating a payment order may occur in different ways; first, the customer may not take the proper procedure to secure the access device or the important information from unlawful access. [30] Secondly, the customer may be negligent in selecting the password or PIN code by choosing obvious numbers or letters, for example, the customer's birthday or name.[31] Thirdly, the customer may not notify the bank "properly and promptly of the loss or theft of the access device." [32] Lastly, the customer fails to notify the bank promptly and properly of unauthorised payment orders after receiving from the bank a notification of fund transfers. [33] Thus, the customer's delay in notifying the bank may prevent the bank from quick recourse against the wrongdoer, due to the wrongdoer's insolvency or disappearance. Moreover, the delay in notification gives the wrongdoer the ability to continue issuing unauthorised payment orders. [34] Accordingly, the present author's view is that by drawing an analogy between customer's duty to exercise reasonable skill and care in drawing cheques with the customer's duty to exercise reasonable skill and care in initiating EFT does not help to determine the originator's liability for fraudulent EFT. Consequently, applying the law of forged cheques to the originator and originator's bank's liability for

[28] Geva 2001, note 8 supra at p.394.
[29] ibid.
[30] ibid.
[31] ibid.
[32] ibid.
[33] ibid.
[34] ibid.

fraudulent EFT leads to unpredictability and uncertainty in their liability. Therefore, there is strong reason to agree with Geva who asserts that

> " [A]n analysis focusing on causality or degree of fault may be hopelessly unpredictable and unsatisfying. The distinct nature of electronic authentication .....makes the case law dealing with handwritten signature authentication not particularly helpful" [35]

In *Tai Hing Mill Ltd.* v *Liu Chong Hing Bank Ltd.* and others [36] it was held that the customer was not negligent and was not under any duty to inspect the bank statement and to notify the bank of the forged cheque. [37] The customer is under such duty if there is a "a conclusive evidence clause" [38]in the contract, which states and specifies in clear language, that the customer must inspect the bank statement and notify the bank of forged cheques. Otherwise the bank is not entitled to debit the customer's account as a result of forged cheques. In this case Lord Scarman stated:

> "[I]f banks wish to impose upon their customers an express obligation to examine their monthly statements and to make those statements, in the absence of query, unchallengeable by the customer after expiry of a time limit, the burden of the objection and of the sanction imposed must be brought home to the customer." [39]

By analogy, the originator is under no duty to inspect the bank statement to determine whether there are unauthorised EFT and notify the bank promptly, unless such a duty is stipulated expressly in the contract and brought to the attention of the customer.[40] The present author's view is that in the absence of such express duty in the bank contract, the originator's bank's right to debit the originator's account depending on authenticated EFT, is uncertain. This is because the originator's bank is unable through electronic means to

---

[35] ibid, at p. 397.
[36] *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd,* note 23 supra, considered by *Hiron v Pynford South,* [1992] 28 E.G. 112 (QBD (OR)) and *Cemp Properties (UK) Ltd v Dentsply Research & Development Corp (No.1),* [1989] 35 E.G. 99 (Chd).
[37] *Tai Hing Mill Ltd,* ibid at p. 81.
[38] ibid at p. 95.
[39] ibid at p.110
[40] Geva 2001, note 8 at p.401 and Hooley and Taylor, note 7 supra at p.133.

detect if the authenticated payment order is in fact an authorised payment order or not. Meanwhile, the originator is under no duty to check periodic bank statements and notify the bank about an unauthorised payment order. Such a situation increases the banks' vulnerability and liability for authenticated but unauthorised payment orders, which means that they may be unable to recover the money due to fraudster insolvency or disappearance. Therefore, the cost and speed of executing payment orders may be affected, due to the uncertainty and unpredictability of the banks' liability for an authenticated but unauthorised payment order. Unpredictability and uncertainty causes instability in determining the parties' liabilities and rights in the short and long term, in particular for the originator's bank. The originator can at any time sue the originator's bank for authenticated but unauthorised debits, even though he was informed about a payment order by sending him a bank statement. This is why Geva rightly argues that

> "[I]n principle, the sender of a payment order ought to be held responsible for the contents of all properly authenticated payment orders, regardless of unauthorised alterations occurring either in the customer's own organisation or in a third party communication system employed by the customer. This conclusion is supported by the general law of agency." [41]

In *London Joint Stock Bank v Macmillan and Arthur* [42] the House of Lords demonstrated the duties the customer should exercise with reasonable care and skill. [43] The House of Lords in *London Joint Stock Bank v Macmillan and Arthur* accepted *Young v Grote* as an authority for the customer owing his bank a duty to draw his cheques with reasonable care so as to prevent forgery. [44] In *London Joint Stock Bank v Macmillan and Arthur,* a firm, entrusted to a confidential clerk, whose integrity they had no reason to suspect, the duty of filling in their cheques for signature. The clerk presented to one of the partners of the firm

---

[41] Geva 2001, note 8 supra at p.400.
[42] *London Joint Stock Bank, Limited v Macmillan and Arthur*,[1918] A.C.777 approved by *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd. and others* [1986] A.C.80 and applied by *National Bank of New Zealand v Walpole and Patterson,* [1975] 2.N.Z.L.R.7.
[43] *London Joint Stock Bank,* ibid, at p.789.
[44] ibid, at p.784.

for signature a cheque drawn in favour of the firm or bearer. There was no sum in words written on the cheque in the space provided for the writing and there was the figure "2.0.0" in the space intended for figures. The partner signed the cheque. The clerk subsequently added the words "one hundred and twenty pounds" in the space left for words and wrote the figures "1" and "0" respectively on each side of the figure "2," which was so placed as to leave room for the introduction of the added figures. The clerk presented the cheque for payment at the firm's bank and obtained payment of 120l from the firm's account. The House of Lords held that the firm had been guilty of a breach of special duty arising from the relations between banker and customer in taking care when drawing the cheque; that the alteration in the amount of the cheque was the direct result of that breach of duty; and that the bank were therefore entitled to debit the firm's account with the full amount of the cheque. Lord Finlay stated as follows:

> "[I]t is beyond dispute that the customer is bound to exercise reasonable care in drawing the cheque to prevent the banker being misled. If he draws the cheque in a manner which facilitates fraud, he is guilty of a breach of duty as between himself and the banker, and he will be responsible to the banker for any loss sustained by the banker as a natural and direct consequence of this breach of duty." [45]

The House of Lords in this case decided that the customer owed his bank a duty to exercise reasonable care in drawing the cheque in respect of writing and signing the cheque. According to the House of Lords' judgment, the customer is liable for material alteration occurring as a result of the customer's negligence in drawing the cheque. The House of Lords refused to impose any wider duty on the customer to exercise reasonable care and skill. [46] There is every reason to agree with Wadsley, Penn [47] and Geva [48] who assert that English case law, such as *Young v. Grote* and *London Joint Stock Bank Ltd* v *Macmillan* imposes a narrow duty on the customer towards his bank to exercise reasonable care and

---

[45] ibid at p. 789.
[46] ibid, at p. 799-801, Geva 2001, note 8 supra at p. 399 and Wadsly and Penn, note 25 supra at p.242.
[47] Wadsly and Penn, ibid.
[48] Geva 2001, note 8 supra at p.399.

skill. According to case law, firstly the customer does not owe his bank a duty to exercise reasonable care in carrying on business, including selecting employees, so as to detect or prevent forgeries. [49] In *London Joint Stock Bank Ltd* v *Macmillan* Lord Finlay emphasised that the customer does not owe his bank a duty to exercise reasonable care in selecting his employees. Lord Finlay stated as follows

> "[O]f course the negligence must be in the transaction itself, that is, in the manner in which the cheque is drawn. It would be no defence to the banker, if the forgery had been that of a clerk of a customer, that the latter had taken the clerk into his service without sufficient inquiry as to his character. Attempts have often been made to extend the principle of Young v. Grote beyond the case of negligence in the immediate transaction, but they have always failed."[50]

Secondly, the customer does not owe his bank a duty to exercise reasonable care to protect and secure the cheques or corporate seals. [51] Thirdly, the customer does not owe his bank a duty to exercise reasonable care to inspect the bank statement to discover the forged cheques and to notify the bank in order to avoid future forgeries.[52] Further, the narrow duty the customer owes to his bank to exercise reasonable care and skill is affirmed in *Kepitigalla Rubber Estates v. National Bank of India*[53] . Here, the court held that

> "(I)t seems to me to be clearly the duty of a person giving a mandate to take reasonable care that he does not mislead the person to whom the mandate is given..... to afford a defence to the banker the breach of duty must be, as in Young v. Grote, in connection with the drawing of the order or cheque, and that there is no obligation as between customer and banker that the person should take precautions in the general carrying on of his business or in examining and checking the pass-book." [54]

Wadsley and Penn confirm that according to case law, which provides a narrow duty of the customer towards his bank, it is unclear when a customer's action in drawing and signing a

---

[49] ibid.
[50] *London Joint Stock Bank, Limited v Macmillan and Arthur,* note 42 supra at p. 795.
[51] Geva 2001, note 8 supra at p.399.
[52] ibid.
[53] *Kepitigalla Rubber Estates v. National Bank of India,* [1909] 2K.B1010 applied by Brewer v Westminster Bank, Ltd [1952] 2 All E.R.571.
[54] *Kepitigalla Rubber Estates,* ibid at p.1022.

cheque is deemed to be serious negligence or not.[55] By analogy, if the payment order in the context of EFT is altered by one of the originator's employees after an authorised person has issued the payment order, it is uncertain whether the originator's bank is entitled to debit the originator's account or not. The present author's view is that the originator's bank should be entitled to debit the originator's account in the above mentioned situation as long as the payment order is authenticated, regardless of whether it is an authorised payment order or not. Furthermore, the present author argues that in the context of EFT, it is inappropriate to discharge the originator from exercising reasonable care in carrying out his business or securing the computer terminal and the passwords or PIN number from being accessed by an unauthorised person. Furthermore, the originator must owe his bank a duty to exercise reasonable care to inspect the bank statement and inform the bank about unauthorised payment orders. The present author justifies this argument as follows: in the context of EFT, the alteration of the payment order by a fraudster may occur by gaining access to the computer terminal as a result of the originator's negligence. Moreover, the alteration may occur by a fraudster who obtains the PIN number or password as a result of the originator's negligence in carrying on his business. Thus, with respect to an electronic payment order the originator's bank receives electronic instructions which appear on a computer screen. Then the originator's bank verifies the payment order by using reasonable security procedures. Once the payment order has been authenticated, the bank regards the payment order as an authorised payment order and transfers the money. The originator's bank is unable to determine whether the person who sends the payment order is authorised to do so or not. Accordingly, if such unauthorised person alters the payment order as a result of the originator breach of his duty to exercise reasonable care to safe and secure the computer terminal, or the PIN code or the password from unlawful access, the originators

[55] Wadsly and Penn, note 25 supra at p.242.

must be liable for fraudulent EFT and the originator's bank must be entitled to debit his account. Geva confirmed that

> " (Y)et, the point is uncertain, and it may well be that in English law there is no customer's duty to prevent unauthorized electronic funds transfer, just as there is no customer's duty to prevent the forgery of his signature." [56]

However, Geva provides a convincing argument that the bank can argue before the court, namely that the customer is under an implied duty to exercise reasonable care and diligence to prevent unauthorized EFT, founded on two points: first, the bank is unable to determine whether an authorized or unauthorized person has issued the authenticated payment order, as the bank receives the payment order through electronic means. Secondly, according to common law, there are mutual and reciprocal duties imposed on them towards each other.[57] It means as much as the bank owing its customer a duty to exercise reasonable care and skill in implementing and maintaining the security of the system. Consequently, the customer owes his bank reciprocal duty to prevent the unauthorised initiation of unauthorised electronic funds transfer. [58]

In conclusion, in the absence of any particular rules governing EFT in England, the originator's bank and the originator's liability for fraudulent EFT are solved by applying the general principles of law; mostly by drawing an analogy with the law governing loss allocation in case of forged cheques. [59] Applying the law of forged cheques to the originator and the originator's bank's liability for fraudulent EFT leads to unpredictability and uncertainty in their liability, as is demonstrated in this section. Further, unless an express contract exists between the originator's bank and the originator, it seems that the

---

[56] Geva 2001, note 8 supra at p.400.
[57] ibid.
[58] ibid.
[59] ibid, at p. 393 and Robert Pennington, "Fraud, Error and System Malfunction: A Lawyer's Viewpoint," Royston Goode, *Electronic Banking: The Legal Implications,* Institute of Bankers, London, 1985 at p. 67.

customer is not under any duty to exercise reasonable care and diligence in the following situations. First, the customer is not under a duty to inspect periodic bank statements in order to detect and notify the bank promptly of unauthorized EFT. [60] Secondly, the customer is not under duty to protect the security of the computer terminal in order to prevent the initiation of unauthorized EFT. [61] Thirdly, the customer is not under duty to exercise reasonable care in the ordinary course of carrying on business, such as selecting the employee, so as to detect or prevent the initiation of unauthorized EFT. [62]

### 4.3.2 The Originator's Bank's Liability for Fraudulent EFT as a Result of its Negligence

In England the originator's bank has a duty to exercise reasonable care and skill in carrying out the customer's instruction to transfer money in the context of EFT. [63] Thus, the originator's bank is under a duty to adhere to the customer's payment order. [64] However, a problem may arise when the customer's instructions are ambiguous, and the bank's execution of that payment order is not in compliance with customer's instructions as a result of the ambiguity. [65] The doctrine of strict compliance applies in the context of different types of transactions that the bank may execute on behalf of its customer. The doctrine of strict compliance has been alleviated in the context of funds transfer orders. [66] In *Royal Products Ltd* v *Midland Bank Ltd* the plaintiff alleged *inter alia* that the doctrine of strict compliance which applies to documentary credit transactions should be applied in

---

[60] *Tai Hing Mill Ltd.* v *Liu Chong Hing Bank Ltd.*and others, note 23 supra.
[61] Geva 2001, note 8 supra at p.399 and *London Joint Stock Bank, Limited v Macmillan and Arthur*, note 42 supra.
[62] *London Joint Stock Bank, Limited v Macmillan and Arthur*, ibid and Geva 2001, ibid.
[63] *Royal Products Ltd* v *Midland Bank Ltd*, note 4 supra.
[64] ibid and Ellinger, Lomnicka and Hooley, note 21 supra at p.549.
[65] Hooley and Taylor, note 7 supra at p.120.
[66] *Royal Products Ltd* v *Midland Bank Ltd*, note 4 supra.

respect of money transfer when the originator's bank executes the originator's payment order. [67] The court disagreed with the plaintiff, as Webster J stated

> " [I] reject the submission also if by it he means that in construing those instructions I should, as a matter of law or banking practice, give a legal implication to each detail of them, for it seems to me that the doctrine which would lead to that result has little application to the facts of the present case, having received its first authoritative recognition Equitable Trust Co. of New York v. Dawson Partners Ltd.,....in the context of confirmed credits. It may be that that doctrine has been or should be applied to all documentary credits; but the transaction in this case is not a 'documentary credit' within the meaning of that expression contained in the Uniform Custom and Practice for Documentary Credits." [68]

Webster J. held that the doctrine of strict of compliance that applies in documentary credit has no application in respect of money transfer, and the originator's bank did not breach the customer mandate. [69] Furthermore, the bank is not breaching its duty to exercise reasonable care and skill in carrying out the customer mandate as long as the bank's actions comply with current banking practices. [70] Moreover, the customer owes his bank a duty not to facilitate fraud. Thus the customer should issue a clear and unambiguous payment order. [71] Devlin J. in *Midland Bank Ltd.* v *Seymour* [72] has emphasised that "the instruction to the agent must be clear and unambiguous." [73] According to case law such as *Midland Bank Ltd.* v *Seymour*, the originator's bank does not breach its duty to exercise reasonable care and skill in executing the customer's payment order whenever the originator's bank proves that it has adopted a reasonable interpretation of the customer's unclear and ambiguous payment order. [74]

The present author's view is that in the context of EFT, the originator's bank is more concerned with the authentication of the payment order than the content of the payment

---

[67] ibid, at p.199.
[68] ibid.
[69] ibid.
[70] ibid, at p.205.
[71] ibid.
[72] *Midland Bank, Ltd.* v *Seymour,* [1955] 2 Lloyd's Report.147.
[73] ibid, at p. 168.
[74] ibid, Hooley and Taylor, note 7 supra at p.120 and *Royal Products Ltd* v *Midland Bank Ltd,* note 4 supra.

order. Accordingly, when the originator's bank debits the originator's account, depending on an authenticated payment order that has been verified by reasonable security procedures, even if it is an unauthorised payment order, the originator's bank can argue that it has performed its duty to exercise reasonable care and skill in carrying out the customer's mandate. However, according to case law, if the originator managed to prove that the originator's bank knew or should have known that the payment order was ambiguous, the court may hold that the originator's bank is negligent and acted unreasonably if it did not ask for clarification from the originator. [75] As Goff L.J states:

> "....even in the context of agency and other analogous transactions,..... in our judgment, that a party relying upon his own interpretation of the relevant document must have acted reasonably in all the circumstances in so doing. If instructions are given to an agent, it is understandable that he should expect to act on those instructions without mercy; but if, for example, the ambiguity is patent on the face of the document it may well be right (especially with the facilities of modern communications available to him) to have his instructions clarified by his principal, if time permits, before acting upon them." [76]

In determining whether the originator's bank exercised its duty with reasonable care and skill in the context of ambiguous payment order, Hooley and Taylor emphasise that the following issues are of importance to the court: firstly, whether the originator's bank interpretation for the customer's payment order is reasonable; [77] secondly, how clear and patent the ambiguity of the payment order is; and [78] finally, whether the originator has the time and the ability to communicate with the originator to ask for clarification before executing the payment order. [79] In the absence of particular rules governing fraudulent EFT these, factors are helpful in determining the originator's bank liability for an ambiguous payment order in the context of authenticated but unauthorised EFT. Nonetheless, these factors do not solve the problem of the unpredictability and uncertainty

---

[75] *European Asian Bank A.G. v. Punjab and Sind Bank* [1983] 1 Lloyd's Rep.611 referred to by *Minories Finance v Afribank Nigeria Ltd*, [1995] 1 Lloyds's Rep. 134 (QBD (comm.)).
[76] *European Asian Bank A.G,*. ibid, at p.618.
[77] Hooley and Taylor, note 7 supra at p.121.
[78] ibid.
[79] ibid.

of the originator's bank liability for authenticated but unauthorised payment order. This is because the bank's liability for authenticated but unauthorised EFT depends on the court's interpretation as to whether the bank has executed its duty with reasonable care and skill or not.

Moreover, the originator's bank owes the originator a duty of care and skill not to facilitate fraud whenever the bank is on notice that the customer's agent is misappropriating his principal's money. [80] In such a case, the paying bank's duty of care not to facilitate fraud conflicts with its duty to adhere to the customer's mandate, which is issued according to the customer's mandate. [81] Thus, in *Barclays Bank* v *Quincecare* [82] Steyn J. held that a banker must refrain from executing an order if he is "put on enquiry," in the sense that he has reasonable grounds for believing that the order is an attempt to misappropriate the customer's funds. [83] The originator's bank liability for misappropriation of the customer's funds depends on the facts of the case. For instance in *Barclays Bank* v *Quincecare* the chairman of the company fraudulently misappropriated the company's funds by instructing the bank over the phone to transfer £344,000 from the company's account to a firm of solicitor's accounts. The bank refused to transfer money until the chairman had sent a written payment order. The bank was authorised to carry out instructions in writing signed by two executive directors or the chairman alone. Accordingly, the bank transferred the funds to the solicitor's account, and the money was transferred to the chairman's account in the USA, who in turn disappeared with the funds.

The company brought an action against the bank alleging that the bank breached its duty of care and skill by transferring the funds. The court held that the bank did not breach its duty

---

[80] Hapgood, note 11 supra at p. 413 and Hooley and Taylor, note 7 supra at p.124
[81] ibid.
[82] *Barclays Bank Plc* v *Quincecare Ltd,* [1992] 4 All E.R. 363 at p. 376.
[83] ibid at p. 376.

of care and skill because the bank received a valid and authenticated payment order. Besides, the bank knew the chairman for a period of time that made him reliable, and the chairman answered the bank's inquiry that the company wished to purchase four chemist shops. Hapgood persuasively argues that the court decision in *Quincecare* and *Lipkin Gorman* v *Karpnale Ltd.*[84] are instrumental in establishing the scope of duty of care that the paying bank owes to his customer. He further argues that both case adopted rational standard of the contractual duty that owes by the paying bank to its customer. [85] In *Lipkin Gorman* v *Karpnale Ltd.* [86] Parker L J demonstrated the standard of care the bank owed its customer in carrying out the payment orders given by the chairman on behalf of the company, is determined as follows

> "[T]he question must be whether if a reasonable and honest banker knew of the relevant facts he would have considered that there was a serious or real possibility albeit not amounting to a probability that his customer might being defrauded. ...That at least the customer must establish. If it is established, then in my view a reasonable banker would be in breach of the duty if he continued to pay cheques without enquiry. He could not simply sit back and ignore the situation." [87]

It should be borne in mind that in EFT, the originator's bank receives the payment order through electronic means, and vast numbers of payment orders need to be executed at high speed. The originator's bank is not able to determine whether the person who sends the payment order is acting on his own behalf or misappropriating the originator's money. It is useful to mention here that the originator's bank is more concerned with the authentication of the payment order than its content. The present author's view is that in fraudulent EFT, where the sender of the payment order is acting on his behalf or misappropriating the originator's money, the originator's bank should not be held liable for such an unauthorised payment order, provided the payment order has been verified by reasonable security procedures.

---

[84] *Lipkin Gorman* v *Karpnale Ltd*, [1989] 1W.L.R.1340.
[85] Hapgood, note 11supra at p.415.
[86] *Lipkin Gorman* v *Karpnale Ltd,* note 84 supra at p. 1378.
[87] ibid, at p.1378.

Furthermore, the originator's bank is liable for a fraudulent payment order was occurred by an agent or employee that the bank employs to accomplish the money transfer. [88] The originator's bank is liable for its employees' negligence or fault acts which are executed while carrying out the customer's payment order. [89] If the bank's employees, in the course of their work or out of their course of work, execute or assist in a fraudulent payment, the originator is entitled to sue the bank to recredit his account. [90] In regards to the bank's agent the originator's bank owes the originator a duty of care and skill to employ a reliable intermediary bank to accomplish funds transfer transaction. [91] Under common law the originator's bank is liable for the intermediary bank negligence or default in executing the funds transfer. [92] This is understandable because mostly in EFT, the intermediary bank is chosen by the originator's bank, and not by the originator. Accordingly, there is a contractual relationship between the originator's bank and the intermediary bank, where such relationship does not exist between the intermediary bank and the originator. Consequently, the originator cannot sue the intermediary bank directly for negligence in carrying out the funds transfer, as there is no contractual relationship between the originator and the intermediary bank. [93] Instead, the originator can sue the originator's bank if the funds transfer is not completed as a result of fraudulent actions occur as a result of the intermediary bank's negligence. [94] In the leading case on this legal point, *Royal Products Ltd* v *Midland Bank Ltd,* Webster J. held that Royal Product (originator) could not sue National Bank (intermediary bank) for negligence, for the reason that the National bank has executed the funds transfer as an agent to the Midland Bank (originator's bank),

---

[88] Wadsly and Penn, note 25 supra at p. 374.
[89] Pennington, note 59 supra at p.76.
[90] ibid.
[91] Wadsly and Penn, note 25 supra at p.374 and Ellinger, Lomnicka and Hooley, note 21 supra at p. 499.
[92] Wadsly and Penn, ibid and Ellinger, Lomnicka and Hooley, ibid at p.500.
[93] See *Royal Products Ltd* v *Midland Bank Ltd*, note 4 supra. Wadsly and Penn, ibid at p.375.
[94] Wadsly and Penn, ibid.

not as an agent to the Royal Product (originator). [95] He further argued that the National Bank does not owe the Royal product a duty of care and skill and the National Bank owes such duties to the Midland Bank.[96] Webster J. stated as follows:

> "[B]ut in my judgment National owed no duty of any kind direct to Royal Products. Although Midland were entitled, as Royal Products later admitted, to execute the instructions by using the services of National as their correspondents, Royal Products had given Midland no authority which would have had the effect of creating privity of contract between them and National,..... In my judgment, therefore, National are not to be regarded as having been agents of Royal Products and did not, therefore, owe them any of the duties, including a fiduciary duty, owed by an agent to his principal." [97]

Therefore banks, mostly in their standard term contracts, exclude liability for negligence of their intermediary banks that engaged to carry out the funds transfer.[98] Such an exclusion clause in respect of business customers might be found reasonable clause according to the case law and the Unfair Contract Terms 1977. [99] An example from case law is that of *Calico Printers' Association, Ltd. v. Barclays Bank, Ltd* [100]. The claimant's large company delivered to Barclays Bank bills of exchange payable at sight and drawn upon merchants in Beirut with regard to goods consigned there. It was agreed that Barclays Bank should warehouse and insure the goods against fire if they were not taken up. Barclays bank instructed intermediary bank in Beirut, but that bank did not insure the goods. When a large fire occurred in the Customs House in Beirut the goods were destroyed, but it was found that no insurance had been affected. The words in the plaintiffs' advice note to Barclays Bank were: "If goods are not taken up, please do your best on our behalf to warehouse and insure them against fire." Barclays Bank, who denied any breach, relied on

---

[95] *Royal Products Ltd* v *Midland Bank Ltd*, note 4 supra at p.198.
[96] ibid.
[97] ibid.
[98] Wadsly and Penn, note 25 supra at p. 375, Hooley and Taylor, note 7 supra at p.126 and Xavier Thunis, "Recent Trends Affecting The Banks' Liability During Electronic Funds Transfer," J.I.B.L. 1991, 6 (8), 297-309 at p.229.
[99] Unfair Contract Terms Act 1977 section 3(1) and *Calico Printers' Association, Ltd.* v *Barclays Bank, Ltd* [1931] 39 LI.L.Rep.51.
[100] *Calico Printers' Association, Ltd. v Barclays Bank, Ltd* [1931] 39 LI.L.Rep.51.

the following provision, which, they said, protected them: "Collections are undertaken at depositors' risk only, on the understanding that no liability whatever attaches to the bank in connection therewith or with the storage and insurance of the relative goods." Lord J. Scrutton held that such clause exempted Barclays bank from liability for the intermediary bank negligence for not insuring the goods. [101] Accordingly, the originator bank can avoid liability for fraudulent EFT occuring as a result of the intermediary bank's negligence in carrying out the customer's payment order. In such a situation the originator cannot recover the money back as he cannot sue the originator's bank because of an exclusion clause. At the same time he cannot sue the intermediary bank because of the lack of the contractual relationship between them.

In regards to business customer under s.3 of the Unfair Contract Terms Act 1977 such an exclusion clause might be found to be a reasonable clause. Hooley and Taylor have explained that the basis of such reasonableness exists, in that the originator bank cannot control the acts of its agent and the business customer is expected to insure against risk. [102] Accordingly, Hooley and Taylor provide a convincing argument that the originator has two means to bring an action against the originator's bank for fraudulent EFT executed as a result of the intermediary bank negligence. [103] First, the originator should prove before the court that the originator's bank has breached its duty of care and skill in employing an unreliable bank. [104] Such a claim is not easy to establish, especially if the bank has chosen a reputable bank. [105] Second, the originator should convince the court that the clause is unreasonable, according to the Unfair Contract Terms Act 1977. [106] Section 11(1) states that:

---

[101] ibid, at p.58.
[102] Hooley and Taylor, note 7 supra at p.126 and See Ellinger, Lomnicka and Hooley, note 21 supra at p. 500.
[103] Wadsly and Penn, 25 note supra at p. 375.
[104] ibid and Hooley and Taylor, note 7 supra at p.127.
[105] ibid.
[106] Wadsly and Penn, ibid at p.375.

> " [I]n relation to a contract term, the requirement of reasonableness for the purposes of this Part of this act, ...is that the term shall have been fair and reasonable one to be included having regard to the circumstances which were, or ought reasonably have been known to or in the contemplation of the parties when the contract was made."

In the light of this section, the unreasonableness of the exclusion term differs from one case to another, depending on the facts of the case. For example, the originator can argue the he could not negotiate the exclusion clause with the originator's bank because there was no equal bargaining power when they signed the contract. [107] Furthermore, the originator may argue that the originator's bank is the only one to transfer money to the required destination. Therefore it may have had had no choice but to submit to the terms of the contract.[108] In conclusion the present author's view is that the originator's bank can avoid liability for fraudulent EFT executed as a result of the intermediary bank's negligence by stipulating an exclusion clause in the contract. Such a clause is likely to be a reasonable one, as mentioned above, according to the case law and the Unfair Contract Terms Act 1977.

Further, the originator's bank owes its customer a duty to exercise reasonable care and skill in employing and activating reasonable security procedures and making sure that its equipment is working effectively. [109] Such security procedures should be reasonable and effective to prevent an unauthorised payment order being initiated or altering an authorised payment order by getting unlawful access to the computer system or intercept the bank-customer's communication. [110] Hooley and Taylor rightly argue that if the bank supplies its customer with hardware or software programmes, the bank is under an implied duty to

---

[107] Ewan Mckendrick, *Contract Law* 5[th]ed, Palgrave Macmillan, Basingstoke, 2003, p.248.
[108] ibid.
[109] Pennington, note 59 supra at p.77, Geva, note 8 supra at p. 397 and Hooley and Taylor, note 7 supra at p.125.
[110] ibid.

supply its customer with reasonable and effective programmes. [111] Any bank which does not supply its customer with such adequate equipment or programmes is breaching its contractual duty in exercising reasonable care and skill. [112] Moreover, Hooley and Taylor have argued that the banks' liability for breaching such duty does not necessarily prove that the bank is negligent.[113] Moreover, Geva argues that the originator's bank that employs reasonable security procedures to authenticate the customer's mandate might be entitled to debit the customer's account as long the security procedures operate properly. [114] Geva continues by arguing that where security procedures are found to be inadequate and ineffective to detect unauthorised payment order and the customer was not found negligent, the bank should be liable for the loss. [115] Azzouni asserts that the bank is the party which chooses and decides on the security procedures to authenticate the payment order, not the customer. Therefore the bank must be liable for the security procedures' imperfections. [116] However, the problem of loss allocation may arise where neither the bank nor its customers are negligent. In such a case, which party bears the liability for the fraudulent payment order which is executed by a third party? Is it the bank or its customer? Moreover, which party bears the liability if both the bank and its customer are negligent? Or is the customer alone found to be negligent?

Geva has argued that depending on the parties' "causality or degree of fault" to determine the parties' liability in the above-mentioned cases, it might lead to unpredictable and uncertain liability for both parties. [117] Besides, applying case law is not helpful, as case law deals with hand writing authentication procedures is inadequate when applied to electronic

---

[111] Hooley and Taylor, ibid.
[112] ibid and Geva 2001, note 8 supra at p.397.
[113] Hooley and Taylor, ibid.
[114] Geva 2001, note 8 supra at p.397
[115] ibid.
[116] Azzouni, Ahmed, note 6 supra at p.362.
[117] Geva 2001, not 8 supra at p. 397.

authentication procedures. [118] Therefore, Geva argues that there is no certain answer to the parties' liability for fraudulent payment order, when both of them are negligent or neither of them is negligent. [119] Geva has stated as follows:

> " [I]n fact, in addition to the degree of adequacy or reasonableness of the security procedures implemented by the bank(that is, the standard of care the bank is required to meet), the question of the customer's negligence, but only in a situation where the bank was negligent as well, remains uncertain. Thus, even where the unauthorized payment order has been properly authenticated, where both the customer and the bank were at fault, question arises as to how the loss is to be apportioned between the bank and the customer according to their respective degree of fault, whether the loss is nevertheless allocated to one of the parties, or whether an elusive search for the party primarily responsible, that is, for the proximate or immediate cause to the loss, should be launched. So far, no definite answer has been provided." [120]

Accordingly, the originator and the originator's bank liability for fraudulent payment order need, to be more certain and predictable for both parties because the predictability and the certainty of the liability encourages the originator's bank to execute the payment order at high speed, low cost and effectively. Therefore the originator and the originator's bank's rights, duties and liabilities need to be regulated by particular rules devoted to EFT. Such rules should take into consideration the distinctive nature of the payment order in EFT, which is authenticated by using security procedures incomparable with the methods are used to authenticate written payment order. The present author argues that the UK Regulations and the EU Directive need to be amended by adding rules regulating the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. Such rules should contain the minimum standards of the rules of the UNCITRAL Model, which regulates the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. These rules will be examined in the next chapter.

---

[118] ibid.
[119] ibid at p.398.
[120] ibid.

## 4.4.DAMAGES RECOVERABLE FROM THE ORIGINATOR'S BANK IN FRAUDULENT EFT

### 4.4.1 Direct Damages

In England, there is no statute or case law to regulate recoverable damages in EFT, except the UK regulations which apply to EFT up to 50,000 Euros. Since, the relationship between the originator and the originator's bank is a contractual relationship, the originator's bank liability for damages can be determined by applying the general principles of contract law. In England, there is consensus [121] that the purpose of the award of damages is to compensate the innocent party for the loss suffered as a result of the other party's breach of contract. [122] Parke B. in *Robinson v. Harman* [123] stated as follows: " the rule of the common law is, that where a party sustains a loss by reason of a breach of contract, he is, so far as money can do it, to be placed in the same situation with regard to damages as if the contract had been preformed." [124] When the originator's bank debits the originator's account on the strength of the fraudulent EFT, the originator bank might breach its contractual duty to adhere to customer instructions. The originator's bank's breach of duty triggers its liability for damages the originator sustains as a result of debiting his account and crediting the fraudster's account. Such damages are direct damages, consequential damages and interest loss. Arora asserts that

> " [T]he measure of damages recoverable by the customer of paying bank [in electronic credit transfer] [125] if that bank fails to carry out the customer's instructions properly because of negligence, will be the measure generally applicable in a breach of contract, ie compensation for such loss as is reasonably

[121] Donald Harris, David Campbell and Roger Halson, *Remedies in Contract & Tort* 2nd ed, Butterworths, London, 2002 at p. 74, Mckendrick, note 107 supra 403 and Wadsley p.215 and McGregor, Harvey, *McGregoer on Damages* 17thed, Sweet & Maxwell, London, 2003 at p. 186.
[122] ibid.
[123] *Robinson v. Harman* (1848) 1 Ex 850 referred to in list of authoritites by *Jackson and Another v Royal Banl of Scotland,* [2005] UKHL 3 and *Panatown Ltd v Alfred McAlpine Construction Ltd*, [2000] 4 All ER 97.
[124] *Robinson,* ibid at p.855.
[125] The words in square brackets added.

> foreseeable as a consequence of a breach of kind in question. This is not necessarily confined to the amount of the payment that should have been made, or to the amount of the payment which was incorrectly made. Thus, where a paying bank wrongfully dishonours a cheque drawn by a customer whose commercial reputation may be adversely affected, the customer can recover for the additional injury caused to him." [126]

In fraudulent EFT, the originator loses the principal amount of money which the originator's bank debits from his account as a result of an unauthorised payment order. Moreover, the originator will not be able to use that amount of money for his own business purposes because it is not in his account anymore. Accordingly, the originator may lose favourable contracts or sustain financial loss as a penalty for late payment. [127] Further, the originator will lose the interest he would have been paid for that the amount of money if it was still in his account. [128] The originator may also lose the fees he paid to the originator's bank to transfer the money to a specific beneficiary but the money instead is transferred to a fraudster. As mentioned earlier in this section that the measure of damages for breach of contract applies to the originator's bank's liability for damages in fraudulent EFT. Accordingly, "so far as money can do it," [129] the originator should be put in the same position he would he have been in, had his account been not debited or his payment order been transferred to the required beneficiary. [130] The application of this measure is restricted by the remoteness rule of *Hadley v. Baxendale.* [131] Alderson B. states as follows:

> "[W]here two parties have made a contract which one of them has broken the damages which the other party ought to receive in respect of such breach of contract should be such as may fairly and reasonably be considered arising naturally, i.e., according to the usual course of things, from such breach of contract itself, or such as may reasonably to have been in the contemplation of the both parties, at the time they made the contract, as the probable result of the breach of it." [132]

---

[126] Arora 1997, note 1 supra p.146.
[127] ibid and Ellinger, Lomnicka and Hooley, note 21 supra at p. 503.
[128] Ellinger, Lomnicka and Hooley, ibid.
[129] *Robinson v. Harman*, note 123 supra and Mckendrick, note 107 supra p.248.
[130] ibid.
[131] *Hadley v. Baxendale* (1854) 9 Exch 341. This case was confirmed by the Court of Appeal in *Victoria laundry (Windsor) Ltd v. Newman Industries Ltd* [1949] 2 KB 528 and applied *by Amstrad Plc v Seagate Technology Inc*, [1998] Masons C.L.R. Rep. 1
[132] ibid, at p. 354.

According to *Hadley v. Baxendale*, the damages that can be recovered for breach of contract are divided into two rules. [133] Firstly, the innocent party can recover the damages "arising naturally" as a result of breaching such contract. Mckendrick explains that the damages which arise naturally, the damages which there is a "serious possibility" or a "real danger" or a very "substantial probability" that such loss would occur as a result of breaching the contract. [134] Secondly, the innocent party can recover the damages which do not a rise "naturally" if such damages were in the both parties' contemplation when they entered the contract. [135]

In the light of the first rule of *Hadley v. Baxendale*, it seems reasonable to suggest that the courts will consider the following losses as "arising naturally" as a result of executing fraudulent EFT. Firstly, the originator's bank must refund to the originator the amount of money specified in the fraudulent payment order. Secondly, the originator's bank must refund the expenses and fees the originator pays to the originator's bank to transfer the money to the required beneficiary. Finally, the originator's bank must pay the interest of the principal sum of money which is debited from the originator's account until the day the originator's bank re-credits the originator's account.

[133] ibid, Harvey McGregor, *McGregoer on Damages* 17th ed, Sweet & Maxwell, London, 2003, at p.187 and Mckendrick, note 107 supra at p. 424.
[134] ibid.
[135] ibid.

### 4.4.2 Consequential Damages

The originator may sustain consequential damages as a result of the originator's bank execution of fraudulent EFT, as debiting the originator's account deprives him from using the amount of money that has been debited from his account to enter, perform or conclude contracts. Consequential damages may arise such as a cancellation or losing an important contract because of late payment or losing the opportunity to enter into tender or buy cheap shares. [136] According to the second rule of *Hadley v. Baxendale*, consequential damages are not recoverable unless they "may reasonably to have been in the contemplation of the both parties, at the time they made the contract, as the probable result of the breach of it."[137] Where the originator's bank knows that its failure to carry out the originator's payment order incurs special losses for the originator in such situations, the originator is entitled to recover consequential damages. [138] In *Simpson v. London and North Western Railway CO* [139] and *Seven Seas Properties Ltd v. AL-Essa* [140] the court held that the defendant's liability for consequential damages arose from the defendant's awareness of the special circumstances that caused the claimant's losses. [141] In contrast, if the defendant is not aware of such special circumstances, the customer is not entitled to recover consequential losses. Furthermore, in *Horne v. Midland Railway* [142] the majority of judges found that it is insufficient for the claimant to draw the defendant's attention to special circumstances. The claimant must go further, to establish that the defendant accepted liability for the consequential losses. [143] Arora asserts thus:

---

[136] Arora 1997, note 1 supra p.147 and Ellinger, Lomnicka and Hooley, note 21 supra at p. 503.
[137] *Hadley v. Baxendale,* note 131 supra at p. 354.
[138] *Simpson v. London and North Western Railway CO* (1876) 1 QBD 274 and *Seven Seas Properties Ltd v. AL-Essa* (No.2) [1993] 1 WLR 1083).
[139] ibid.
[140] *Seven Seas Properties Ltd v. AL-Essa,* note 138 supra.
[141] ibid and *Simpson v. London and North Western Railway,* note 138 supra.
[142] *Horne v. Midland Railway*(1872-1873) L.R. 8 C.P. 131.
[143] ibid, at p. 135-142 and 146-148.

> " ...unless the paying bank is made aware of the essential character of the prompt payment when it accepts the customer's instructions, the bank will not normally be liable for special loss which its customer suffer because the payment is essential to secure a contract he is negotiating... . If the bank is unaware of the need for prompt payment, the paying bank will not be liable to compensate its customer for the loss he suffers as a result of any special circumstances which necessitated the prompt payment." [144]

McKe ndrick explains that courts experience great difficulty in determining whether the loss has been in the parties' reasonable contemplation when they entered the contract. [145] In *Victoria Laundry (Windsor) Ltd v. Newman Industries Ltd* [146] the Court of Appeal confirmed that the defendant's knowledge of the special circumstances was either imputed or actual. Imputed knowledge is the knowledge of the reasonable man who is deemed to know that losses arise from a breach of contract in ordinary circumstances. [147] The losses arising under imputed knowledge are covered by the first rule of *Hadley v. Baxendale.* Meanwhile, the actual knowledge is the awareness of special circumstances beyond the "ordinary course of things" where losses resulting from a breach of contract are covered by the second rule of *Hadley v. Baxendale.* In regards to EFT, Arora argues that such payments are usually used to discharge commercial transactions. Therefore, the originator's bank might be considered to be aware of the possibility that the originator will suffer some commercial losses if the payment order is not performed properly. [148] Further, Arora argues that the originator must be entitled to recover the damages which usually arise as a result of commercial payment not being paid. However, Arora confirms that it is not easy to calculate the "usual commercial loss" as the courts have not yet decided how such losses should be calculated. [149]

---

[144] Arora 1997, note 1 supra p.94
[145] Mckendrick, note 107 supra at p. 423.
[146] *Victoria laundry (Windsor) Ltd v. Newman Industries Ltd* [1949] 2 KB 528, CA.
[147] ibid, at p.539-540.
[148] Arora 1997, note 1 supra p.94.
[149] ibid.

The present author's view is that in wholesale EFT, although the originator' s bank knows that the originator utilises payment orders to discharge commercial transaction, this does not imply that the originator's bank is aware of the consequential damages the originator may sustain if the payment order not being performed properly. Moreover, it should be taken into consideration that in EFT transactions, the originator's bank receives a vast number of payment orders from the originator. These payment orders should be executed at high speed, so it is not possible for the originator's bank to predict the consequential damages for every payment order. Therefore, according to the second rule of *Hadley v. Baxendale*, the originator's bank should be aware of the consequential damages that the originator may sustain if the payment order is not being performed properly. Moreover, the originator's bank must be aware of such potential consequential damages at the time of entering into the contract, if the consequential damages of some EFTs exceed the damages which are brought to the attention of the originator's bank at the time of entering into the contract. In such a situation, at the time of giving the instruction, the originator should bring to the attention of the originator's bank any potential consequential damages that may result if this transaction is not performed properly.

All in all, there is uncertainty in the originator's bank liability for consequential damages under common law rules, in particular the *Hadley v. Baxendale* rule, since it is not easy to distinguish between "imputed knowledge" and "actual knowledge" in order to determine whether the originator's bank is liable for the consequential damages or not. [150] McGregor asserts that there is no " rigid division between the "first rule" and the "second rule" [*Hadley v. Baxendale*], [151] and that the modern re-statement of the rule as totality is a

[150] Mckendrick, note 107 supra at p. 423 and McGregor, note 136 supra at p. 200.
[151] The words in square brackets added.

salutary trend." [152] The uncertainty and unpredictability of the originator's bank liability for consequential damages hinders the originator's bank from carrying out the originator's payment order at high speed and low cost. Moreover, as mentioned before, the originator's bank, in its standard term contracts, excludes or limits its liability for fraudulent EFT executed as a result of the intermediary bank's negligence. Under English common law, the originator cannot sue the intermediary bank as there is no privity in contract between them. This leaves the originator unable to recover either the direct damages or the consequential damages from both banks. Therefore, the present author argues that the originator's bank's liability for the direct damages and consequential damages should be regulated by particular rules devoted to EFT. This can be achieved by amending the UK Regulations on Cross-Border Credit Transfer, which will be discussed in the next section.

[152] McGregor, note 133 supra at p.201.

## 4.5. THE FAILURE OF THE EU DIRECTIVE AND THE UK REGULATIONS TO REGULATE LIABILITY FOR FRAUDULENT EFT

This section examines the originator's bank and the originator's liability for fraudulent EFT under EU Directive and the UK Regulations on cross-border credit transfer. Furthermore, this section demonstrates the Jack Committee Report 1989 view on the bank-customer's liability for fraudulent EFT and the need for particular rules to regulate such liability.

### 4.5.1 The Originator's Bank's Liability for Late and Failed Payment Orders under the EU Directive and UK Regulations on Cross-Border Credit Transfers

The EU Directive on Cross-Border Credit Transfer was influenced by the UNCITRAL Model Law on International Credit Transfer. [153] However, the EU Directive and the scope of UK Regulation are more limited when compared to the Uncitral Model Law, for the following reasons. Firstly, the Uncitral Model Law applies to international credit transfers, while the EU Directive and the UK regulations do not apply to credit transfers executed between parties in countries outside the EU. Secondly, the UNCITRAL Model Law may apply to inter-bank credit transfers but the EU Directive and the UK regulations do not apply to such credit transfers. Thirdly, the UNCITRAL Model Law applies to large-value credit transfers without pecuniary limits, whereas, the EU Directive and the UK regulations apply to credit transfer up to 50.000 Euros. However, neither the UNCITRAL Model Law nor EU Directive and UK regulations apply to domestic or international debit transfers.

[153] Lotte Bojer, "International Credit Transfers: The Proposed EC Directive Compared with the UNCITRAL Model Law," J.I.B.L. 1995, 10 (6), 223-228 at p.233.

There is every reason to agree with Bojer who asserts that the EU Directive is not a sophisticated, nor comprehensive instrument like the UNCITRAL Model Law. [154] The present author agrees with Bojer because the EU Directive does not regulate some of the problems which are been regulated under the UNCITRAL Model Law. For instance, the EU Directive does not lay down when a payment order is an authorised payment order or deemed to be an authorised payment order. Furthermore, EU Directive and UK regulations do not regulate the liability of the credit institution (originator's bank) and the originator for fraudulent payment orders, which may be executed by the customer's employees, the bank's employees and a third party. Arora confirmed "[T]he Regulations [UK regulations] do not deal with unauthorised or mistaken transfer orders, completion of payment and revocability of the payment mandate. These issues continue to be governed by the common law."[155]

Accordingly, the present author argues that the EU Directive and the UK Regulations should be amended by adding rules regulating the originator and the originator's bank's liability for a fraudulent payment order. Furthermore, there is a need for rules to be adopted to determine when the payment order is an authenticated payment order and when the payment order is an authorised payment order. Moreover, the EU directive and the UK regulations should contain rules imposing on the bank a duty to implement reasonable security procedures to authenticate the originator's payment order. The EU Directive and the UK Regulations should amend such rules by adopting the minimum standards regarding the rules of the UNCITRAL Model Law, which regulate the originator and the originator's bank's liability for fraudulent EFT.

---

[154] Bojer, ibid at p. 228.
[155] Anu Arora, " Round up: Banking Law," Comp. Law. 2000, 21(8), 234-244, at p. 244.

The EU Directive and UK Regulations impose liability on the credit institution in case of delay or failure to execute the payment order. [156] Under the EU Directive and the UK Regulations, the credit institution is under a duty to transfer money within a limited time as specified by the originator. [157] If there is no time specified, the originator's institution should transfer the money to the beneficiary's account within five banking business days after the day of accepting the payment order by the originator's institution. [158] If the originator's institution fails to transfer money within the required time, regardless of the reason, the originator's institution is obliged to pay interest to the originator. [159] However, the originator's institution is obliged to pay such compensation provided that the delay is not attributable to the originator's fault. [160] Accordingly, if the payment order was delayed as a result of fraudulent actions attributable to the originator's institution, the originator's institution should pay the originator compensation. The originator's institution is obliged to pay the originator only the amount of interest lost, but is not obliged to compensate the originator for any consequential damages he may suffer. [161] However, the originator can sue his institution for such loss according to contract or tort law. [162] Ellinger *et al* emphasise that paying interest for delay by the originator's institution to the originator has affected the originator's institution's liability for delay. They state as follows

> "[T]he Regulation [UK Regulations] alter the position that would otherwise apply at common law. In particular, Regulation 6 provides for the payment of interest to the originator by the originator's bank where a transfer is not made within the relevant time, unless the delay is attributable to the fault of the originator. This gives rise to strict liability on the part of the originator's bank, which is something different from its position at common law where liability turns on its failure to exercise reasonable care and skill in and about the execution of the originator's payment order. The

[156] EU Directive Article 6&8 and UK Regulations, Regulations 6&9.
[157] EU Directive Article 6(1) and UK Regulations, Regulation 6(1) (2).
[158] ibid, Richard Hooley "EU Cross-Border Credit Transfers- the New Regime," B.J.I.B. & F.L.1999, 14(9), 387-395 at p. 391.
[159] EU Directive Article 6(1), UK Regulations, Regulation 6 (3), Hooley, ibid.
[160] EU Directive Article 6(3), UK Regulations, Regulation 6 (5), Hooley, ibid.
[161] Hooley, ibid.
[162] ibid and UK Regulations, Regulation 15(1).

originator's bank can recover any compensation paid to the originator from an intermediary bank which may be responsible for the delay." [163]

Moreover, the originator's institution is entitled to recover compensation from any intermediary bank which is responsible for the delay, even if there is no contractual relationship between them. [164] Hooley explains that the ability to pass the loss through the funds transfer chain down to an intermediary bank which is responsible for the delay is a new concept in banking law.[165] She states as follows "[T]his is a novel concept in this area, as the common law has been slow to short-circuit a contractual chain of liability by the imposition of tortuous duty of care between remote parties." [166]

The originator's institution may fail to transfer funds as a result of fraud. In such a case, the originator seeks to recover the money debited from his account. Under the EU Directive and the UK regulations the originator is entitled to recover the money from the originator's institution according to the "money-back guarantee" rule [167] if the payment order is not completed for any reason. The originator's institution is obliged within fourteen banking days of the originator's request for refund to recredit his account with the amount of money that is debited from his account, plus interest and charges. [168] The liability of the originator's bank to refund the amount of failed credit transfer is limited to 12.500 Euro or its equivalent in EEA currency. [169] Thus, if the originator suffers consequential damages or the amount of the failed credit transfer exceeds 12.500 Euros, he can recover these losses according to contract or tort law. [170] In such a case, the originator should prove that the originator's institution been negligence, as it did not exercise a reasonable care and skill to

[163] Ellinger, Lomnicka and Hooley, note 21 supra at p.555 and Hooley, note 158 supra at p. 391.
[164] EU Directive Article 6(1), UK Regulations, Regulation 7 (6) (7) and Hooley, ibid.
[165] Hooley, ibid.
[166] ibid.
[167] The EU Directive, Article 8, UK Regulations, regulation 9, Ellinger, Lomnicka and Hooley, note 21 supra at p.504 and Hooley, ibid at p. 393.
[168] ibid.
[169] ibid.
[170] Ellinger, Lomnicka and Hooley, ibid and Hooley, ibid at p. 393.

accomplish the originator's mandate. [171] Steennot has criticised the limitation of the originator's institution liability for failed transfer, which is limited to 12.500 Euros. He argues that "there are no good reasons for limiting the liability for 12.500 if the amount of the credit transfer is higher than 12.500 Euro and lower than 50.000." [172] The present author agrees that since the scope of the EU Directive and the UK regulations are limited to the credit transfers up to 50.000, the originator's bank's liability under "money-back guarantee" rule should be limited to the same amount. Given that in England the "money-back guarantee" rule is limited to funds transfers up to 12.500 Euro, the liability of the originator's bank for funds transfer exceeds 12.500 Euro is governed by English common law. This means the liability of the originator's bank for 50.000 Euro fraudulent funds transfer is determined by the UK regulations for the first 12.500 and by English common law for the next 37.500 Euro, which causes confusion and difficulties in determining the liability of the originator's bank. On 29/11/2002 the European Commission and Council of Union promised in its follow up report on the application of the EU Directive to increase the scope of the "money-back guarantee" rule to 50.000 Euro to match with the scope of the EU Directive. [173] However, the scope of the "money-back guarantee" rules still has not been changed during the period of writing this thesis.

Under the EU Directive and the UK Regulations, the originator's institution can recover the refund paid to the originator from the intermediary institution, and the intermediary institution can pass the loss down the chain to the intermediary institution which is responsible for the failed transfer. [174] However, if the funds transfer fails as a result of

---

[171] Ellinger, Lomnicka and Hooley, ibid and Hooley, ibid

[172] Reinhard Steennot, "The Single Payment Area," J.I.B.L.2003, 18(12), 481-487 at p. 485.

[173] European Parliament, the Legislative Observatory, Cross-Border Credit Transfers, Procedure Ended and published in the official Journal.
http://www.europarl.europa.eu/oeil/file.jsp?id=87492
http://www.europarl.europa.eu/ (obtained on 24/12/2006)

[174] The EU Directive Article 8, UK Regulations, Regulation 9, Ellinger, Lomnicka and Hooley, note 21 supra at p.504 and Hooley, note 158 supra at p. 393.

fraudulent action occurring through an intermediary institution chosen by the originator, the originator's institution is not liable to refund to the originator the failed transfer amount.[175] In such a case, the originator's institution is obliged to take reasonable steps to trace and recover the funds. Thus, the originator can take action against an intermediary institution he instructed based on contract or tort law. [176] In this case, the originator will have to prove the negligence of that intermediary institution and it failed to exercise reasonable care and skill to carry out the customer's mandate.

### 4.5.2 The Jack Committee Report's View on the Liability For Fraudulent EFT

The Jack Committee Report was more focused on retail EFT than wholesale EFT, in particular ATM and POST services. However, the Jack Committee Report recognised four major problems related to retail and wholesale EFT transactions in general: first, authentication of payment orders; secondly, security procedures relating to existing systems; thirdly, liability for loss in the case of fraud or system malfunction; and lastly, countermand and reversal of instructions.[177] The following subsection examines the Committee's view on the third problem, as the first and second problems have been examined in previous chapters, and the last problem falls beyond the remit of this study.

The Jack Committee Report was concerned with how the loss should be distributed in case of fraudulent EFT between the bank and the customer, and which party should bear the burden of proof to prove that the payment order is an unauthorised payment order. [178] Thus, the Jack Committee Report examined whether there was a need for regulations which govern EFT to solve the former problems, or whether the contractual approach was

[175] ibid.
[176] The EU Directive, Preamble, UK Regulations, Regulation 15and Hooley, note 158 supra at p. 393.
[177] "Review Committee on Banking Services: law and practice," report by the Review Committee/ Chairman: R.B. Jack, Vol. XLIX 622-630, 1989 at p.77.
[178] ibid.

adequate and proper to deal with the loss allocation and the burden of proof. [179] The Jack Committee Report concluded that there is a need for EFT rules; the need for such rules was justified as follows:

> " (I)t is difficult not to conclude, from this brief survey of the arguments on either side [one side was against the new rules and the other side was for the new rules], that there is a pressing need for EFT to be subject to some degree of regulation. The Review Committee at least is persuaded of this view. Leaving EFT solely to contractual arrangement does not appear to meet the case, when there is widespread doubt as to whether the allocation of duties and liabilities among the providers and users of EFT systems is totally equitable. The arguments against any sort of regulation have been shown to be partly suspect and, for the rest, less than conclusive." [180]

Moreover, the Jack Committee Report made recommendations for loss allocation as a result of fraud. The majority of these recommendations were devoted to customer-activated system. [181] However, the present author's view is that there is no reason not to take such recommendation into consideration in the context of wholesale EFT, as both wholesale and retail EFTs are executed through electronic means. The Jack Committee Report recommended that a statutory law should apply in order to apportion loss allocation between parties in cases of fraud. Moreover, the rules of such statutory law should be mandatory rules. Thus the parties' liability for fraudulent EFT cannot be varied by the parties' agreement. [182] The apportionment of loss liability should take in consideration the contribution of parties' acts in causing fraudulent EFT. Furthermore, the Jack Committee Report stated as follows:

> " (A)apportionment of the loss should take into account such factors as(i) the steps taken by the customer to protect the security of his card and PIN, (ii) the extent to which the system provided by the bank protects the customer against unauthorised transactions on his account, and (iii) the relative weight of the evidence adduced by the parties in support of their respective contentions that the transaction was, or was not, authorised." [183]

---

[179] ibid, at p.78.
[180] ibid, at p.81.
[181] ibid atp.93.
[182] ibid, at p.94.
[183] ibid, at p.95.

With respect to wholesale EFT, the former factors might be taken in consideration to apportion liability for loss, by examining whether the customer has protected their computer terminal and PIN from unauthorised access. Moreover, the reasonableness of the security procedure employed by the bank should be taken in consideration to apportion the parties' liability.

## 4.6. CONCLUSION

In conclusion, in England, the parties' duty to exercise reasonable care and skill in initiating and carrying out electronic payment orders plays a significant role in determining the parties' liability for fraudulent EFT. Depending on such a duty to determine the parties' liability has led to uncertainty and unpredictability in determining the parties' liability. The uncertainty of liability exists as result of applying forged cheque rules to fraudulent EFT, as the rules govern paper-based payment orders' problems are not adequate to deal with electronic payment order problems. This is attributed to the difference in the means used to initiate and authenticate payment orders in each case. In cheques, the payment order is a written payment order and authenticated by verifying the customer's signature, whereas in EFT, the payment order is initiated electronically and authenticated by security procedures. As mentioned earlier, UK Regulations need to be amended by adding rules which regulate the parties' liability for fraudulent EFT. Moreover, such rules should impose on the bank a duty to implement reasonable security procedures, so as to authenticate the originator's payment order. The EU Directive and the UK Regulation are not comprehensive and sophisticated instruments, for many reasons: firstly, the scope of application, as they are applied to credit transfers up 50.000 Euro. Secondly, their provisions do not deal with the

authorisation and authentication issued of EFT, which are instrumental factors to allocate the loss between the parties.

The Jack Committee recognised that there is a need for a statutory law for EFT and the contractual approach is neither efficient, nor sufficient to deal with retail or wholesale EFT problems: specially, the problem of loss allocation between parties in case of fraudulent EFT. The Jack Committee recommended adopting mandatory rules for loss allocation as a result of fraud, and the apportionment of loss should take into consideration the contribution of parties' acts.

The present author argues that particular rules devoted to EFT are needed to regulate and govern the parties' liability for an unauthorised payment order, as the parties' liability under the English common law is uncertain and unpredictable. Geva rightly argues that the rules that may be adopted to govern the parties' liability for unauthorised payment order should take into consideration *inter alia* the following issues: firstly, the peculiarity of EFT payment orders that are initiated and authenticated by using electronic means; [184] secondly, the rules should impose a duty on the bank to employ reasonable security procedures; [185] thirdly, the rules should impose on the customer to secure and protect his or her PIN or computer terminal from unauthorised accesses. [186] Fourthly, the customer should not be liable for an unauthorised payment order if he is not at fault, even if the bank is not at fault either. [187] In such a case, the bank should be liable, as the bank can redistribute the loss between its customers. Moreover, this will encourage the bank to improve its security procedures. [188] Finally, the rules should take into account the customer's fault in executing an unauthorised EFT, otherwise the customer will not use/take the required steps to protect

[184] Benjamin Geva, "Unauthorised Electronic Funds Transfers Comparative Aspects," Ziegel, Jacob S. (ed), *New developments in international commercial and consumer law:* proceedings of the 8th Biennial Conference of the International Academy of Commercial and Consumer Law, Hart, Oxford, 1998 at p. 132.
[185] ibid.
[186] ibid.
[187] ibid.
[188] ibid.

their PIN or terminal from unlawful access. [189] The next chapter examines the UNCITRAL Model Law and Article 4A schemes in distributing the liability for fraudulent EFT between the originator and the originator's bank. Furthermore, the next chapter demonstrates that the originator and the originator's bank liability for fraudulent EFT are more predictable and certain than under the English common law.

[189] ibid.

# CHAPTER FIVE

# PARTIES' LIABILITY FOR FRAUDULENT WHOLESALE EFT UNDER THE UNCITRAL MODEL LAW AND ARTICLE 4A

## 5.1.INTRODUCTION

The previous chapter concluded that under English contract law and agency law, establishing the originator and the originator's bank's liability for fraudulent wholesale EFT remains uncertain and unpredictable. Moreover, UK Regulations and EU Directive are not comprehensive and sophisticated legislation, as they are limited in application, and do not regulate the originator and the originator's bank's liability for fraudulent wholesale EFT. Accordingly, the present author's view is that the UK Regulations and the EU Directive need to be amended by adding rules to regulate the originator and the originator's bank liability for fraudulent wholesale EFT. Such rules should contain the minimum standard of the rules in the UNCITRAL Model Law and Article 4A.These rules regulate the originator and the originator's bank's liability for fraudulent EFT more effectively and efficiently, because they make the originator's and the originator's bank's liability for fraudulent wholesale EFT more predictable and certain.

This chapter evaluates the rules of the UNCITRAL Model Law and Article 4A, which regulate the originator and the originator's bank's liability for fraudulent EFT. This chapter will demonstrate that the originator and the originator's bank's liability for fraudulent EFT under such laws are more predictable and certain when compared to

English contract law and agency law. This chapter will conclude by suggesting that the rules on fraudulent EFT in the UNCITRAL Model Law and Article 4A should be adopted as minimum standards to regulate the originator and the originator's bank' liability for fraudulent EFT under the UK Regulations and EU Directive. Accordingly, these rules will be examined from two dimensions, that is, the rules of the UNCITRAL Model Law on fraudulent EFT and those of Article 4A on fraudulent EFT. This is because the UNCITRAL Model Law has been influenced heavily by Article 4A. While the UNCITRAL Model Law is a model law for the countries to take it into consideration when they enact their national laws. Article 4A is currently applies in USA therefore it can be used as an example to illustrate the application of a law that might adopt the rules of the UNCITRAL Model Law.

The present author's view is that the UNCITRAL Model Law and Article 4A allocate the bank-customer's liability for fraudulent EFT by considering four main issues: first, the authentication of payment orders; secondly, authorised and unauthorised payment orders; thirdly, the parties' liability for unauthorised payment orders executed by variant fraudsters; and lastly, the "money-back guarantee" [1] rule. The first and second issues are examined extensively in chapters two, three and four, under English law, the UNCITRAL Model Law and Article 4A respectively. This chapter considers the third and fourth issues under the UNCITRAL Model Law and Article 4A. Moreover, this chapter examines the originator's duty to notify the

1 UNCITRAL Model Law in International Credit Transfer 1992, art. 14
http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf (obtained 03/02/2004)
and Article 4A of the Uniform Commercial Law 1989 s. 204. (Hereafter Article 4A)
http://www.law.cornell.edu/ucc/4A/overview.html#PART%201 (obtained 03/02/2004)
http://www.ali.org/

originator's bank about unauthorised payment orders, according to the "Statue of Repose" [2] under Article 4A. Such a duty will be examined to demonstrate how the originator and the originator's bank's liability are more predictable and certain under Article 4A. The significance of this duty, which does not exist under the UNCITRAL Model law, and its effect on the parties' rights, will be examined subsequently in this chapter. Section 5.2 of this chapter examines the originator and the originator's bank's liability for fraudulent EFT under the UNCITRAL Model Law. While Section 5.3 evaluates the originator and the originator's bank's liability for fraudulent EFT under Article 4A. Both sections 5.2 and 5.3 of this chapter examine the rules of article 4A and UNCITRAL Model Law as follows: firstly, these sections demonstrate the significance of the parties' agreement on the security procedures that should be employed to authenticate the originator's payment orders. Further, these sections demonstrate how the parties' agreement affects the parties' liability for fraudulent wholesale EFT. Secondly, Sections 5.2 and 5.3 examine the originator and the originator's bank's liability for fraudulent EFT, when the payment order has been executed by the originator's employees, the originator's bank's employees and a third party. These sections demonstrate that the originator and the originator's bank's liability for fraudulent wholesale EFT is determined depending on the person who issued the unauthorised payment order. Thirdly, Sections 5.2 and 5.3 continue by analysing the originator's banks liability for direct damages, consequential damages and interest. These sections elaborate the fact that the originator's bank's liability for such damages are limited and can be predicted by the originator's bank and originator when they agree to transfer funds by using electronic means. Fourthly, sections 5.2 and 5.3 examine the originator's basis for action against the originator's bank and

[2] The official Comment on Article 4A issued by The American Law Institute (ALI) and The National Conference of Commissioners on Uniform State Law (NCCUSL), 1989, (1) of U.C.C s. 4A-505. (Hereafter the Official Comment to the U.C.C).

freedom of contract. These sections demonstrate that freedom of contract under the rules of the UNCITRAL Model Law and Article 4A has limitations in protecting the originator from unfair contract terms. As mentioned earlier, Article 4A imposes a duty on the originator to notify the originator's bank about unauthorised payment orders, according to the "Statute of Repose." This duty will be discussed under section 5.3.5 only, as such a duty does not exist under the UNCITRAL Model Law.

## 5.2. THE RULES OF THE UNCITRAL MODEL LAW ON FRAUDULENT EFT

Article 5 of the UNCITRAL Model Law makes no distinction between the originator and originator's bank's liability for fraudulent EFT, whether the unauthorised payment order is issued from the start by a fraudster, or by the originator, and is then altered or amended later by a fraudster. [3] According to Article 5 of the UNCITRAL Model Law, there are two factors of significance that affect the originator's bank's and the originator's liability for fraudulent EFT: firstly, whether there is an agreement between the originator and the originator's bank as to the security procedure that should be employed to authenticate the originator's payment orders; secondly, whether the fraudster who issues the payment order is one of the customer's employees, or the bank's employees, or a third party.

[3] The UNCITRAL Model Law art. 5 (1) and (2)

### 5.2.1 The Significance of the Parties' Agreement on the Security Procedures

Under Article 5 of the UNCITRAL Model Law the parties' agreement on the security procedures in the contract is significant to allocate the risk between the originator and the originator's bank for fraudulent payment order. [4] According to Article 5(1) of the UNCITRAL Model Law, the rules of agency are applied to determine the liability of originator's bank for fraudulent payment order under two circumstances; firstly: if there is no agreement between the originator's bank and the originator on the security procedures that should be applied to authenticate the electronic payment order; and [5] secondly, if the authentication procedure used to authenticate the payment order is a "mere signature." [6] Whether the person sending the payment order is authorised by the originator to send such payment order will be determined by applying the rules of the applicable agency law not by the UNCITRAL Model Law.[7] For example if the applicable law is English agency law, the originator's bank cannot debit the originator's account on the strength of a payment order having been authenticated but not been authorised.

Whereas under Article 5 (2), if there is an agreement between the originator's bank and the originator on the security procedures to be applied to authenticate the

---

[4] Eric E. Bergsten, "A Payment Law for the World: UNCITRAL Model Law on International Credit Transfers," Robert C. Effros, (ed), *Payment Systems of the World*, Oceana Publications, New York, London, 1996 at p. 443 and UNCITRAL, "International Credit Transfer: Comments on the Draft Model Law on International Credit Transfer: Reports of the Secretary-General" (A/CN.9/346), UNCITRAL yearbook, vol. XXII, 1991, p.52-102, at p.64. ( Hereafter Report of the Secretary-General 1991).
http://www.uncitral.org/pdf/english/yearbooks/yb-1991-e/yb_1991_e.pdf
http://www.uncitral.org (obtained on 12/12/2005).

[5] Bergsten 1996, ibid and Report of the Secretary-General 1991, ibid.

[6] Bergsten 1996, ibid and Report of the Secretary-General 1991, ibid.

[7] Report of the Secretary-General 1991, ibid.

payment order, [8] the originator's bank is entitled to debit the originator's account for the payment order that has been authenticated but not been authorised.[9] Under the UNCITRAL Model Law, as a general rule, the originator's bank is not liable for fraudulent EFT issued by an unauthorised person, as long as the payment order has been authenticated. [10] Accordingly, under the UNCITRAL Model Law the originator's bank is entitled to debit the originator's account depending on an authenticated payment order, whether the payment order is in fact authorised or not. Meanwhile, in England, by applying the rules of agency law and by analogy with the rules governing forged cheques, the originator's bank is liable for the payment order that has been authenticated but not authorised. Therefore, under the rules of agency law, the originator's bank is not entitled to debit the originator's account owing to an unauthorised payment order, even if it is authenticated. Applying the rules of agency law to the originator's bank liability hinders the bank from executing the electronic fund transfer at high speed and at low cost, the main characteristics of EFT.[11] In EFT, the originator's bank receives the payment order through an electronic device. Consequently the bank cannot determine whether that the person who sends the payment is authorised or not. Thus, the originator's bank will be reluctant to execute an authenticated payment order at high speed until it is certain that the payment order is authorised. Moreover, the bank may increase the cost of the EFT service, because it is uncertain, and cannot predict whether the electronic payment order is an authorised payment order and the limits of its liability for damages.

---

[8] Report of the Secretary-General 1991, ibid and Bergsten 1996, note 4 supra at p.444.
[9] Bergsten 1996, ibid and Report of the Secretary-General 1991, ibid.
[10] The UNCITRAL Model Law art. 5 (2) and Bergsten 1996, ibid.
[11] Luc Thevenoz, "Error and Fraud in Wholesale Funds Transfers: U.C.C. Article 4A and The UNCITRAL Harmonization Process," 42 Ala. L. Rev.881, Winter, 1991, p.938.

The present author's view is that the UK Regulations and the EU Directive should be amended by adding particular rules regulating the originator and the originator's bank's liability for an electronic authenticated payment order that has not been authorised. Such rules should contain the minimum standard of article 5 (1) and (2) of the UNCITRAL Model Law. This is because under UNCITRAL Model law, the originator and the originator's liability for such payment order is more predictable and certain. Moreover, adopting such rules protects the originator from unfair contract terms that the originator's bank includes in its contract to exclude or limit their liability for fraudulent EFT. Bhala rightly argues thus:

> "[A]rguably, the system '(international payment system)' must have three salient features: it must be certain (i.e. reliable), efficient (i.e., high speed, low cost, and high security), and fair (i.e., equitable in its apportionment of liability). That is, large amounts of funds must be transmitted at low cost and with high security, and the rights and obligations of parties to the wire transfer must be allocated in a fair manner. Accordingly, a legal framework for a wire transfer system is essential to ensuring that all three features are present in the system."[12]

Malaguti provides a convincing argument as to why the bank–customer agreement is not effective in ensuring that EFT is executed at high speed, low cost and remains an ineffective way, for the following reasons. Firstly, Malaguti has argued that the bank-customer agreement is formed in such a way that the originator bears the losses for any fraudulent payment order, as long as it is not executed by the bank's employees.[13] As was demonstrated in Chapter four [14] such an exclusion clause in respect of business customers might be found reasonable according to the English case law and

---

[12] Raj Bhala, "International Payments and Five Foundations of Wire Transfer Law," Essays in International Financial & Economic Law No, 2, International Finance and Tax Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, University of London, in cooperation with the London Centre for International Banking Studies and the London Institute of International Banking, Finance and Development Law, London, 1996 at p. 7.

[13] Maria C, Malaguti, "Legal Issues in Connection with Electronic Transfers of Funds," L.C. & A.I. 1992, 1(3), 275-290 at p. 284.

[14] See Chapter four s. 4.3.2.

the Unfair Contract Terms 1977. [15] The present author is of the opinion that adopting such an approach to apportion liability for fraudulent EFT is unfair, because this means that the non-negligent originator will be liable for third party fraud. Secondly, banks' agreements have adopted different approaches to allocate the loss of fraudulent EFT between themselves and their customers. This agreement approach in allocating the parties' liability for fraudulent EFT has added further confusion and uncertainty to the originator and the originator's bank's liabilities. Patrikis *et al* argue thus:

> "[C]ontractual resolutions, while on occasion able to resolve individual funds transfer disputes, also lacked the uniformity necessary to aid the funds transfers as a whole. Different contracting parties reach different accords. Unequal bargaining power between the contracting parties also significantly weakens the ability of contract law to provide system-wide solutions on case by case approach." [16]

Thirdly, Baker and Brandel persuasively believe that the uncertainty of the parties' rights and obligations of funds transfer is not resolved by contracts defining those rights and duties.[17] This explains why some banks and their customers are reluctant to sign an agreement to determine their liability for possible losses, which may occur as a result of improper execution of the funds transfer. [18] Baker and Brandel emphasized that "As a result, these services have often been used without agreement on key liability issues or without any signed agreement at all." [19] Therefore, the present author argues that particular rules are needed to regulate the originator and the originator's bank's liability for an authenticated payment order that not been

---

[15] Unfair Contract Terms Act 1977 section 3 (1) and *Calico Printers' Association, Ltd.* v *Barclays Bank, Ltd* [1931] 39 LI.L.Rep.51.
[16] Ernest T. Patrikis, Raj K. Bhala and Micheal T. Fois, " An Overview of United States Funds Transfer Law," Robert C. Effros, (ed), *Payment Systems of the World*, Oceana Publications, New York, London, 1996 at p. 6.
[17] Donald I. Baker and Roland E. Brandel, *The Law of Electronic Fund Transfer Systems: Legal and Strategic Planning,* revised edition, Warren, Gorham & Lamont, Boston, 1996 at p.13-4.
[18] ibid.
[19] ibid.

authorised, and should not be left entirely to the contractual approach. It is unarguable that freedom of contract is very important to conclude commercial transactions. However, the present author argues that rules are needed to regulate the above-mentioned parties' rights, and duties should contain some mandatory rules which cannot be varied by parties' agreement to provide protection for both parties. Consequently, if the parties are aware that there are mandatory rules to protect their rights and duties, the originator will not be reluctant to use EFT to pay his obligations and the originator's bank will not be apprehensive in executing EFT at high speed and at low cost.

### 5.2.2 The Originator's and the Origintor's Bank's Liability for Fraudulent EFT Executed by Variant Fraudsters

Chapter three has demonstrated that the general principal under the UNCITRAL Model Law that originator's bank can debit the originator's account depending on authenticated payment order whether it is authorised or not. However, there are two situations where the originator's bank is not entitled to debit the originator's account on the strength of authenticated but unauthorised payment order. According to article 5(4) of the UNCITRAL Model Law, these two situations are when the authenticated but unauthorised payment order is issued by one of the originator's bank's employee, and when such payment order issued by a third party who does not gain access through the fault of the originator or as a result of his relationship with the originator. Thevenoz argues that allocating liability for authenticated payment order has not been authorised according to the person who may initiate such payment order can be justified on the basis that is each party is in the best position to protect his security

procedures. [20] Therefore, the originator and the originator's bank should take all the necessary procedures to protect the information, the devices and the employees related to the security procedures from being accessed or tampered with by unauthorised person. [21] The present author believes that allocating the liability for such payment order according to the person who initiated it is an efficient and fair policy. On one hand, it protects the originator from unfair contract terms, and on the other hand, encourages the bank to employ the most advanced and sophisticated security procedure available in the market to avoid liability.

French provides different categories of persons who may initiate the unauthorised payment order, thus:

> "[T]he universe of individuals who can initiate unauthorised payment orders can be divided into three categories: (1) the "customer shop," (2) the receiving bank's shop" and (3) third parties not associated with either the customer or the bank. The category of third parties can be divided further into two subcategories: A) third parties obtaining access to information or facilities from the customer, and B) third parties obtaining access to information or facilities from the receiving bank." [22]

Assume a hypothetical example that corporation X has a bank account with bank Y. There is an agreement between Bank Y and X on the security procedures that should be used to authenticate X's payment orders. Bank Y has received an electronic payment order from X to transfer £2 million to Z's account in bank Q. Y bank verified the payment order and found that the payment order is an authenticated payment order. Subsequently, bank Y transfers the £2 million to Z's account in Q bank. X is informed either by notification from bank Y or by checking the account statement that its account is debited with £2 million. X protests that the payment order was a fraudulent payment order and he never issued such a payment order, or the

[20] Thevenoz, note 11 supra at p. 941-948.
[21] ibid.
[22] J. Kevin, French, " Article 4A's Treatment of Fraudulent Payment Orders-the Customer's Perspective," 1991, 42 Ala. L. Rev.773 at p. 814.

payment order is altered by fraudsters after it has been issued. It is possible that it could have been issued by one of the customer's employees, or by one of the bank's employees, or by a third party. The next sections examine the originator and the originator's bank liability for fraudulent EFT executed by one of the above-mentioned persons. To demonstrate that the originator and the originator's bank's liability for fraudulent EFT under the UNCITRAL Model Law is more predictable and certain than under English law.

**(a) Fraudulent EFT Executed by Originator's Employees**

According to Article 5(2) of the UNCITRAL Model Law, if the payment order is an authenticated payment order, whether authorised or not, the originator's bank is not liable for such fraudulent EFT. [23] Therefore, if a payment order has been initiated by one of the originator's employees and been authenticated, the originator's bank is not liable for such a payment order, whether the person who issued such payment order was authorised to do so or not. Consequently, under the UNCITRAL Model Law, the originator cannot sue the originator's bank to recredit his account with the amount of money that has been debited from his account, according to fraudulent authenticated payment order. [24] The present author's view is that Article 5(2) of the UNCITRAL Model Law protects the originator's bank as its liability for fraudulent EFT is more predictable and certain. However, Article 5 (2) imposes a duty on the originator's bank in return for such the protection. This is due to the fact that according to Article 5(2) of the UNCITRAL Model Law, the originator's bank is under a duty to

[23] Bergsten 1996, note 4 supra at p.443.
[24] The UNCITRAL Model Law art. 5(2) and Bergsten 1996, ibid, at p. 444.

authenticate the originator's payment order by using "commercially reasonable" security procedures agreed on between the originator and the originator's bank. On the other hand, the originator's bank will not be reluctant to execute the originator's payment order at high speed and low cost, because the originator's bank can predict its liability for an authenticated payment order, regardless of whether it is in fact authorised or not. Accordingly, if the originator's bank wants to make itself immune from the liability for an authenticated payment order that has not been authorised, the originator's bank should make sure that it has employed "commercially reasonable" security procedures. Thevenoz justified the imposition of liability on the originator in such cases, as follows:

> " [S]he [the originator] [25] is in the best position to avoid such losses by taking precautions, like hiring reliable agents, controlling access to sensitive information and areas, and monitoring their use. No persuasive loss- spreading argument can be made since the risk varies mainly with circumstance linked to the purported sender. If the losses were mandatorily shifted to the banks, the banks would price this sort of insurance just as insurers do, by collecting statistical data and fixing premiums according to the customer's own risk profile. This is also consistent with the common sense of equity: corporation should bear the losses suffered because of its officers or through some organizational failure." [26]

In contrast, under English law, by analogy with the rules apply to forged cheques and applying the rules of agency law, the originator can sue the originator's bank to recredit his account with the amount of money debited from his account, according to fraudulent authenticated EFT, on the basis that the fraudulent authenticated payment order is an unauthorised payment order and the originator's bank acted without the customer's mandate. Applying such rules to fraudulent EFT makes the bank reluctant to execute the originator's payment order at high speed, low cost and in an effective way. As the originator's bank's liability under English law for fraudulent EFT is

[25] The words in square brackets added
[26] Thevenoz, note 11 ibid, at p. 942-943.

unpredictable and uncertain, English law rules are ineffective and inadequate in dealing with the originator and the originator's bank's liability for fraudulent EFT. The present author's view is that the originator and the originator's bank's liability for such payment order should be regulated by specific rules devoted to EFT, which take into consideration the distinctive nature of authenticating EFT and should not be analogised with rules that apply to forged cheques.

Accordingly, the UK regulations and the EU Directive should be amended by adding rules regulating the originator and the originator's liability for an authenticated payment order that has not been authorised. The originator and the originator's bank's liability for such payment order should be regulated by enacting rules similar to Article 5 (2) of the UNCITRAL Model Law. Such rules should stipulate that the originator is liable for an authenticated payment order, whether it is in fact authorised or not. At the same time, such rules should impose a duty on the originator's bank to employ "commercially reasonable" security procedures; otherwise the originator is not liable for authenticated payment orders. Enacting such rules make the originator liable for an authenticated payment order has not been authorised issued by one of his unauthorised employees. This is can be justified on the basis that in the world of electronic communication, the originator's payment orders are issued by using electronic means and the originator's bank is unable to determine whether the person who issued the payment order was authorised to issue such a payment order or not, therefore the originators bank should be able to depend on the security procedures to determine whether to accept the originator's payment order or not. Thevenoz emphasized that

> "[T]his provision [Article 5(2)][27] is based on two policies—certainty in commercial transactions ("finality") and efficiency. Since speed and low cost

[27] The words in square brackets added.

> are principal advantages of electronic funds transfers, bank must be able to reach a quick and reliable decision regarding whether to execute any single payment order. This decision should be final if it is supported by a "commercially reasonable" security procedure. Secondly, the provision assumes as a matter of fact that, so long as banks comply with such procedures, their clients are in the best position to avoid fraud, and it is much less expensive for the clients to take additional precautions." [28]

Consequently, under Article 5 (2) of the UNCITRAL Model Law the originator and the originator's bank's liability for authenticated payment order has not been authorised is predictable and certain. Thus, when the parties enter the contract, they are aware of their duties and liabilities in advance for such payment order. This will encourage both parties to use EFT to transfer funds and promote the completion of commercial transaction at high speed and low cost, which are the main advantages of EFT.

**(b) Fraudulent EFT Executed by Originator's Bank's Employees and a Third Party**

The present author's view is that the UNCITRAL Model law aims to strike a balance in distributing liability for fraudulent EFT between the originator and the originator's bank. This is achieved by distributing the liability for fraudulent EFT. Devoting specific rules, on the one hand, protects the originator from unfair contract terms that the originator's bank includes in its contract. On the other hand, it encourages the originator's bank to execute EFT at high speed, low cost and effectively. Therefore, under Article 5(4) of the UNCITRAL Model Law, the originator can shift back the liability for fraudulent EFT to the originator's bank. [29] Thus, the originator's bank is liable for an authenticated payment order that has not been authorised whenever the

[28] Thevenoz, note 11 supra at p. 938.
[29] Ernest T. Patrikis, Thomas C. Baxter, Jr. and Raj K. Bhala, *Wire Transfers: A Guide to U.S. and International Laws Governing Funds Transfers*, Irwin, Illinois, 1993, at p. 275.

payment order is issued by a person who is either not one of the originator's employees, or not a person whose relationship with the originator enables him to gain access to authentication procedures, or he is a third party who does not gain the access to the authentication procedures through the fault of the originator's.

Moreover, Article 5(4) regulates the bank-customer's liability for fraudulent EFT when the payment order is executed as a result of the originator's fault. For instance, the bank may prove that the originator's negligence makes it easier for a hacker to gain information as to penetrate the security procedures, and initiate an unauthorised payment order.[30] Accordingly, the originator could be estopped through his fault from denying that the originator's bank is entitled to debit his account as a result of fraudulent EFT.

Under Article 5 (4) of UNCITRAL Model Law, the originator owes his bank a duty to keep and protect the sources and the transmitting facilities controlled by him from being accessed by any unauthorised person. Otherwise, the originator will be responsible for any authenticated but authorised payment order that is executed by a fraudster who obtains access through sources controlled by him. In comparison to English agency law, contract law and the rules of forged cheques, the customer does not owe his bank a duty to exercise reasonable care in protecting and securing cheques or corporate seals. [31] Moreover, under English law the customer does not owe his bank a duty to exercise reasonable care in carrying on business, including the selection of employees, so as to detect or prevent forgeries.[32] By analogy, under English law, the originator does not owe his bank a duty to protect and secure the

---

[30] Benjamin Geva, *Bank Collections and Payment Transactions, Comparative Study of Legal Aspects*, Oxford, New York: Oxford University Press, 2001 at p. 405.
[31] Geva 2001, note ibid at p. 399.
[32] *London Joint Stock Bank, Limited v Macmillan and Arthur*,[1918] A.C.777 at p. 795.

sources and transmitting facilities controlled by him.[33] Geva has stated that "[I]n all such cases, a customer who was negligent is neither liable in negligence nor estopped by his negligence from asserting the forgeries." [34]

Consequently, the originator will not be liable for an authenticated but unauthorised payment order initiated by a third party who obtained access to the sources controlled by the originator. The present author argues that the originator's bank will be reluctant to execute EFT at high speed and low cost, due to the uncertainty and the unpredictability of the originator's bank liability for fraudulent EFT, issued as a result of the customer's negligence to protect the sources he controlled. Therefore, the present author argues that in England, the originator and the originator's bank's liability for an authenticated payment order has not been authorised and initiated by one of the originator's bank's employees or by a third party should be regulated by specific rules. The UK Regulations and the EU Directive should contain rules to distribute the liability for such payment order between the originator and the originator's bank. The UK Regulations and the EU Directive should adopt rules containing the minimum standards of Article 5 of the UNCITRAL Model Law. As under Article 5 of the UNCITRAL Model law the originator and the originator's bank's liability for fraudulent EFT are more predictable and certain than is the case under English law.

The purpose of such rules should be to distribute the liability between the originator and the originator's bank for an authenticated but unauthorised payment order, by taking into consideration the distinctive nature of the process used for authenticating electronic payment orders. Moreover, such rules should regulate the originator's duty to keep and protect the information and sources for transmitting payment orders and

---

[33] Geva 2001, note 30 supra at p. 399-400.
[34] ibid 399.

the originator's duty to exercise reasonable care in carrying out business, for instance, by selecting the employees and detecting or prevent forgeries, because the originator is the one who is in the best position to protect the sources he controls. Furthermore, the rules should stipulate that the originator's bank is liable for any payment order that has been authenticated but not been authorised which is initiated by a third party, any other person who does not or did not work for the originator and any other person who does not gain accesses to authentication procedures through the originator's fault.

### 5.2.3 The Originator's Bank's Liability for Damages Against the Originator

As indicated in the foregoing pages, a fraudulent EFT is either initiated originally by an unauthorised person (the fraudster), or is initiated by the originator but the fraudster alters the details after the initiation. In both cases the originator loses the principal amount of money, the interests that the originator might be paid if that amount of money was in his account, and he or she may suffer consequential damages, such as losing a preferable contract. The following pages demonstrate how the UNCITRAL Model Law regulates the originator's bank's liability for damages.

#### (a) The Originator's Bank's Liability for Direct Damages and Interest

Under UNCITRAL Model Law, the originator is entitled to a refund for the principal amount of money of the fraudulent payment order from the originator's bank. [35] The originator's actions against the originator's bank are founded on the contractual

[35] UNCITRAL Model Law, art. 14(1).

relationship and the "money-back guarantee" rule. Under Article 14 (1) of the UNCITRAL Model Law the "money-back guarantee" rule states

> "[I]f the credit transfer is not completed, the originator's bank is obliged to refund to the originator any payment received from it, with interest from the day of payment to the day of refund. The originator's bank and each subsequent receiving bank is entitled to the return of any fund is has paid to its receiving bank, with interest from the day of payment to the day of refund."

The credit transfer may not be completed as a result of a fraudulent alteration to the payment order details, for example, by providing incorrect identification of the beneficiary or the beneficiary's bank to transfer the money to the fraudster. [36] According to the "money-back guarantee" rule, if the credit transfer is not completed as a result of fraud, the originator is entitled to sue the originator's bank for a refund and the originator's bank, in turn, can sue his or her receiving bank. [37] Under the UNCITRAL Model Law, the credit transfer is completed when the beneficiary's bank accepts the payment order for the benefit of the beneficiary. [38] Article 14 of the UNCITRAL Model Law is the "money-back guarantee" rule that was adopted to protect the originator whose credit transfer was not completed. [39] Thus every sending bank is entitled to sue its receiving bank in the chain until it reaches the bank where the fraud was executed. Furthermore, the originator's bank must pay interest on the principal amount as a compensation for the delay, which starts from the day the originator paid for the payment order to the date of refund. [40]

According to Article 2 (m) of the UNCITRAL Model Law, interest is defined as follows "[T]he time value of the funds or money involved, which, unless otherwise agreed, is calculated at the rate and on the basis customarily accepted by the banking community for the funds or money involved." Patrikis *et al* rightly argue that defining

---

[36] Report of the Secretary-General 1991, note 4 supra at p.88.
[37] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p. 300.
[38] Model Law art. 19 (1).
[39] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p. 283.
[40] ibid, at p. 300 and UNCITRAL Model Law, art. 4 (1).

interest is significant, as the definition helps the parties to evaluate and predict the value of liability for their actions. [41] Accordingly, the UNCITRAL Model Law imposes on the originator's bank a strict liability to pay interest for the originator for the delay.

The UNCITRAL Model Law stipulates that the "money-back guarantee" rule is a mandatory rule, and cannot be varied through agreement. However, under the UNCITRAL Model Law, there is an exception which provides that the "money-back guarantee" rule can be varied by agreement. In terms of fraudulent payment orders, the originator's bank may agree with the originator to restrict or exclude the originator's bank's liability.[42] This is when the credit transfer transaction involves a "significant risk" that makes any other prudent bank reject executing such a payment order.[43] Schneider stated as follows:

> "[T]wo considerations convinced the Commission to provide at least for small restriction. First, it was asserted with particular emphasis that the contra productive result of the "money-back guarantee" would be that, in the future, credit institutions would simply reject payment orders directed to certain countries due to the risks involved. Second, it was pointed out that there is a danger that in the case if risky payments, the credit institutions
> would advise the customers to pay by check; here the customer would bear the full risk of delivery. For these reasons, it is now stipulated that in exceptional cases deviation may be made from the mandatory refund obligation. If an international transfer involves special risks, the "money-back guarantee" can be excluded "...when a prudent originator's bank would not have otherwise accepted a particular payment order because of the significant risk involved in the credit transfer." [44]

Thorough examinations of UNCITRAL Model Law provisions show that there is neither a definition of the prudent bank, nor any demonstration of which types of risks are significant. Patrikis *at el* have criticised the language of Article 4(2) of the

---

[41] Patrikis, Baxter, Jr. and Bhala 1993, ibid at p. 247.
[42] ibid.
[43] UNCITRAL Model Law art. 14 (2).
[44] Uwe H. Schneider, " The Uniform Rules for International Credit Transfers Under the UNCITRAL Model Law," Hadding, Walther and Schneider, Uwe H. (eds), *Legal Issues in International Credit Transfers,* Duncker & Humblot, Berlin, 1993 at p. 472.

UNCITRAL Model Law as vague and unclear, because it does not provide the meaning of "prudent bank" or describe what risks are significant. [45] On the contrary Bergsten argues that significant risks arise when the customer wants to transfer money to a bank or country where there are economic or political risks.[46] The present author believes that such risks could be occurred, for example, when the originator instructs the originator's bank to transfer the funds through a specified bank which does not implement the required standard of security procedures to such funds transfer. Moreover, if the originator instructs his bank to transfer funds via a specified country, which is well known with low standards of security procedures, in such a case, the bank may exclude or restrict its liability.

The novelty of the "money-back guarantee" rule, under UNCITRAL Model Law, is that it stipulates strict liability on the originator's bank to refund the principal amount of the funds transfer and the interest to the originator. In contrast, under English contract law, the originator's bank liability is not strict, as the originator's bank may exclude or restrict its liability for fraudulent payment orders. According to the "money-back guarantee" rule the originator knows with certainty, in advance, which party can sue for a refund and on what legal basis. This gives the originator more certainty and encourages him to utilise EFT transactions, as long he knows that if something goes wrong, he can sue a specific party for redress. As indicated, such certainty is not available under English law as banks may exclude or restrict their liability for fraudulent EFT in their contract. Accordingly, the originator cannot sue the originator's bank for a refund. The originator bank's liability to pay the originator interest for delay is strict as well, and the time for compensation is confined. By

[45] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p. 284.
[46] Bergsten 1996, note 4 supra at p.477.

comparison, under English law, the originator bank's liability for interest is uncertain and depends on proving that the originator's bank has breached its duty to exercise reasonable care and skill to execute the originator's payment order.

Bergsten emphasized that the rationale behind the "money-back guarantee" rule to entitle the originator to a refund from the originator's bank is, firstly, that the originator's bank is the party who chooses the routing to transfer money. [47] Secondly, according to the originator's bank's duty of reasonable skill and care, the originator's bank must instruct a reliable bank to transfer money. [48] Lastly, it is easier for the originator's bank than the originator to contact the bank in the foreign country, or to sue that bank if the payment order is not completed, due to the intermediary bank's negligence.[49]

The present author's view is that the UNCITRAL Model Law by the "money-back guarantee" rule aims to provide protection and certainty, as the originator is entitled to sue the originator's bank for a refund. Further, the "money-back guarantee" aims to achieve reasonable balance in liability for both the originator's bank and the originator. Therefore, under the UNCITRAL Model Law, the originator's bank is not obliged to refund the amount of money of fraudulent payment order to the originator where the originator's bank cannot obtain refund from the intermediary bank, which the originator has chosen to accomplish the funds transfer. This is an exception to the "money-back guarantee" rule. Article 14 (3) states as follows:

> "[A] receiving bank is not required to make a refund under paragraph (1) if it is unable to obtain refund because an intermediary bank through which it was directed to effect the credit has suspended payment or is prevented by the law from making the refund. A receiving bank is not considered to have been

[47] ibid, at p. 475.
[48] ibid.
[49] ibid.

> directed to use the intermediary bank unless the receiving bank proves that it does not systemically seek such directions in similar cases. The sender the first specified the use of that intermediary bank has the right to obtain the refund from the intermediary."

Accordingly, when the originator's bank is unable to obtain a refund from an intermediary bank, [50] two conditions should be met to exclude the originator's bank from the liability. Firstly, the fraudulent payment order is executed through an intermediary bank, as specified by the originator. Secondly, the originator's bank must prove that it is used to utilizing or following a different route to transfer money: for example a particular payment system or intermediary bank. [51] If the former conditions are met, the originator should seek a refund from the intermediary bank, which he has specified in the payment order to affect the payment order, [52] since Article 14 (1) and (3) compels the party who employs the intermediary bank to employ a reliable bank. Otherwise he will be liable for fraudulent EFT, which occurs as a result of the intermediary bank's negligence. The present author's view is that the UNCITRAL Model Law policy in the "money–back guarantee" rule under Article 14 (1) and (3) gives both parties more protection and equality.

The originator may face a problem that one of the intermediary banks in the chain has become insolvent; the insolvency of the intermediary bank breaks the chain that the money must pass through to reach the originator. [53] According to Article 14 (4) the "skip over" rule specifies that any receiving bank in the chain can discharge its money-back obligation by "skipping over" the failed bank, thereby the receiving bank can make a refund to any prior sender or the originator directly. [54] Moreover, the

[50] ibid at p. 478 and Report of the Secretary-General 1991, note 4 supra at p. 90.
[51] UNCITRAL Model Law, art. 14 (3) and Report of the Secretary-General 1991, ibid, at p. 90
[52] UNCITRAL Model Law, art. 14 (3).
[53] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p. 302.
[54] ibid.

originator under Article 14 (5) is entitled to ask for a refund from any bank in the chain, which is obliged to make a refund under the "money-back guarantee" rule. However, the originator cannot ask for a refund from a bank that has directly paid a refund to its sender or any other bank in the chain.[55] The bank in the chain that pays a refund to its originator directly is discharged from its obligation to make a refund, under the "money-back guarantee" rule. [56] There is a limitation for the "skip over" rule application, where the application of such a rule affects the receiving bank's rights and obligations under any agreement or funds transfer system. [57]

Bergsten rightly argues that Article 14 (4) and (5) of Article 4A of the UNCITRAL Model Law gives more protection and certainty to the originator in refunding his money, [58] as the originator is entitled to refund his money from any receiving bank in the chain. By comparison, under English law, according to contract law and agency law, the originator is not entitled to sue any receiving bank in the chain and any receiving bank in the chain does not owe the originator a duty in contract and agency law. [59] According to English contract law, there is no privity in the relationship between the originator and any receiving bank in the chain, and under English agency law, any receiving bank in the chain is not an agent of the originator. [60] Accordingly, under English contract law and agency law, the receiving bank is not entitled to make a refund for one of the prior banks in the chain or the originator by skipping over the insolvent bank (its sending bank), because there is no privity in contract between them. Thus, the UNCITRAL Mode Law gives the originator alternatives to get a refund from the other banks in the chain if he is not able to get it from the originator's

---

[55] UNCITRAL Model Law, art.14 (5).
[56] ibid.
[57] UNCITRAL Model Law, art.14 (6).
[58] Bergsten 1996, note 4 supra at p. 479.
[59] See *Royal Products Ltd v Midland Bank Ltd*, [1981]2 Lloyd's Rep.194.
[60] ibid.

bank. Further, the "money-back guarantee" rule provides the originator the protection he needs to get his money back, as this rules is mandatory rule cannot be varied by parties agreement. Freedom of contract and mandatory rules under the UNCITRAL Model Law will be discussed subsequently in this chapter.

**(b)The Originator's Bank's Liability for Consequential Damages**

Under Article 18 of the UNCITRAL Model Law, resort is not permitted to any remedy that may exist outside the UNCITRAL Model Law in respect of the originator's bank's failure to complete the funds transfer. [61] Bergsten rightly argues that in the absence of such exclusive remedy the uniformity that the UNCUTRAL Model Law seeks to achieve may be undermined by resorting to other remedies that exist in other doctrines of law. [62] According to UNCITRAL Model Law, the originator's bank is not liable for the consequential damages which the originator suffers as a result of the bank's failure to accomplish the funds transfer. [63] Thus, the originator's bank is not liable for the consequential damages the originator suffers as a result of fraudulent EFT.

If the parties resort to remedies other than the remedies provided under the UNCITRAL Model Law, the amount of consequential damages for fraudulent EFT might exceed the amount of the funds transfer. Such cases make the originator's bank reluctant to accept funds transfer transactions; or alternatively increase the cost to transfer the funds. Therefore, the UNCITRAL Model Law confines the originator's bank liability for consequential damages for fraudulent EFT in order to promote the

---

[61] Benjamin Geva, *The Law of Electronic Funds Transfers; Global and Domestic Wire Transfers, ACH payments, Consumer Transactions*, Mathew Bender, New York, 1994 at p.4-157.
[62] Bergsten 1996, note 4 supra at p. 487.
[63] UNCITRAL Model Law, art.18 and Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p. 260.

main goals of the UNCITRAL Model Law, which are to execute EFT at high-speed, low cost and in an effective way. Moreover, if the originator's bank cannot predict the extent that it may be held liable for consequential damages, it will be difficult to get insurance to cover such liability. [64] Therefore, Article 18 of the UNCITRAL Model Law eliminates such uncertainty and ambiguity with regard to the limitation of the originator's bank liability for consequential damages in the context of fraudulent payment order.

However, there are two exceptions under Article 18 of the UNCITRAL Model Law which make the originator's bank liable for consequential damages. Article 18 of the UNCITRAL Model Law states that:

> "[N]o other remedy arising out of other doctrines of law shall be available in respect of non-compliance with articles 8 or 10, except any remedy that may exist when a bank has improperly executed, or failed to execute, a payment order (a) with the specific intent to cause loss, or (b) recklessly and with actual knowledge that loss would be likely to result."

Accordingly, the originator's bank liability for failure to execute or for improper execution of the payment order is not limited to the remedies of the UNCITRAL Model Law. Provided that one of the two conditions which are specified in Article 18 are met: either, if the bank acted "with the specific intent to cause loss" or if the bank acted "recklessly and with actual knowledge that loss would be likely to result." [65] In such cases the originator can sue the originator's bank for consequential damages based on other sources of law. The UNCITRAL Model Law Working group has noted that the receiving bank would rarely act recklessly or with intent to cause

---

[64] UNCITRAL, Report of the Working Group on International Payments on the work of its twenty-first session, UNCITRAL yearbook, vol. XXII, 1991, A/CN.9/341), New York,9-20, July 1990 at para.127. ( hereafter UNCITRAL Report of the Working Group on International Payments 1991)

[65] UNCITRAL Model Law, art.18.

improper execution.[66] However, in such a case "it would be unconscionable for the bank not to be responsible for the consequences of its acts." [67] However, the exclusivity of remedies under the UNCITRAL Model Law only applies to the actions that breach the provisions of the UNCITRAL Model law, but not to the actions based on other grounds for instance, common law and equity law.

### 5.2.4 Basis of Action and Freedom of Contract

The UNCITRAL Model Law regulates and governs the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. [68] Also, under Article 4 of the UNCITRAL Model Law, parties can vary their rights and obligations by agreement in regard to funds transfer, unless such variation is prohibited according to the UNCITRAL Model Law provisions. [69] Accordingly, under the UNCITRAL Model Law, the originator can bring action against the originator's bank for fraudulent EFT based on breach of contract and breach of UNCITRAL Model Law provisions. The general rules and the basic strategy of the UNCITRAL Model law is the freedom of contract between the parties of funds transfer. However, there are provisions in the UNCITRAL Model Law which provide that they may not be varied or altered by parties' agreement. Article 4 of the UNCITRAL Model Law states that "(E)except as otherwise provided in this law, the rights and obligations of parties to a credit transfer may be varied by their agreement.' The UNCITRAL Model Law provides that Articles 5(2) and 14 the "money-back guarantee" rule, [70] cannot be varied by the

---

[66] UNCITRAL Report of the Working Group on International Payments 1991, note 64 supra, para.128.
[67] ibid.
[68] The UNCITRAL Model Law art. (4), (5), (14), (17) and (18) and Patrikis, Jr and Bhala 1993, note 29 supra, at p. 249-253.
[69] Patrikis, Jr and Bhala 1993, ibid at p.264.
[70] See Sections 2.3.1, 2.2.1 and 2.1 of this chapter for more detail on these rules.

parties' agreement. [71] Accordingly, the originator's bank's liability to refund the principal amount of fraudulent funds transfer, besides the interest to the originator, cannot be varied by agreement. Furthermore, the originator and the originator's bank liability for an authenticated but an unauthorised payment order under Article 5(2) cannot be varied by agreement. Both Articles 5 (2) and 14 are significant as they allocate the parties' liability for fraudulent EFT between the originator and the originator's bank. These rules contribute significantly to protecting the originator from unfair contract terms and encouraging the originator's bank to execute EFT at high speed and low cost. As under the UNCITRAL Model Law, the originator's bank and the originator's liability for fraudulent EFT are more strict and predictable than the English law because it cannot be varied by the parties' agreement.

Under English law, parties' liability for fraudulent EFT is regulated and governed by contract law and agency law. [72] Banks stipulate different terms in their contract with regard to parties' liability for unauthorised EFT, [73] in such terms they exclude or limit their liability for fraudulent EFT. As demonstrated before in chapter two, [74] that according to the UCTA the business customer is most likely bound by the clauses which limit or exclude the originator's bank's liability for fraudulent EFT, as such clauses might be found reasonable against business customer. Azzouni has argued that depending on freedom of contract, some banks bear the whole liability, while other banks may exclude themselves from the liability completely, and another alternative is that of sharing the liability with the customer. [75] Malaguti argues that

---

[71] Charles L.A Cheng, " The UNCITRAL Model Law on International Credit Funds Transfers," Sing. J. Legal Studies. 538, Dec,1993 at p. 547.

[72] Ahmed Azzouni, "Internet banking and the Law: a critical examination of the Legal controls over Internet banking in the UK and their ability to frame, Regulate and secure banking on the net," J.I.B.L.R. 2003, 18(9), 351-362 at p. 360.

[73] ibid at p. 361.

[74] See Chapter two s.2.3.2.

[75] Azzouni, note 72 supra at p. 361.

mostly, the terms in the bank-customer contract exonerate banks from liability for fraudulent EFT when executed by a third party, [76] in particular, when the bank proves that it has complied with the security procedures and the bank's employees are not involved in the fraudulent action in such cases the originator bears the liability. [77] Malaguti states as follows: "(A)s a result, the client in the fact bears any loss other than losses clearly proved to have been caused by fraud of bank's employees." [78] The present author's view is that such clauses are unfair for the originator; the originator must not bear any liability for third party's fraudulent actions not attributable to him or one of his employees. This is because a third party may execute a fraudulent action by intercepting or breaking down security procedures, and the bank not the customer employs may help the fraudster in breaking down such security procedure. Azzouni argued thus:

> "...it was the banks who decided to introduce the new technology, with its admitted difficulties in security, and they, rather than their customers who has no part in that decision, should shoulder any responsibility for its shortcomings. Therefore, when banks do provide these conditions excluding their liability, they must ensure that they use the best security measures." [79]

Accordingly, the present author's view is that the UNCITRAL Model Law does not leave the originator and the originator's bank's liability for fraudulent EFT entirely to the contractual approach without restrictions. As mentioned earlier in this section, the UNCITRAL Model Law imposes restrictions on the parties' ability to vary their liability for fraudulent EFT by stipulating that Articles 5 (2) and 14 are mandatory rules cannot be varied by their agreement. The mandatory rules protect both parties and make the originator and the originator's bank's liability for fraudulent EFT more predictable and certain. Therefore, the UK Regulation and the EU Directive should be

---

[76] Malaguti, note 13 supra at p. 284.
[77] ibid.
[78] ibid.
[79] Azzouni, note 72 supra at p.361.

amended by adding mandatory rules regulating the originator and the originator's liability for fraudulent EFT, to make the originator and the originator's liability for fraudulent EFT more practicable and certain.

## 5.3.ARTICLE 4A of the UCC'S TREATMENT OF FRAUDULENT EFT

It is useful to recall that Article 4A of the UCC has significantly influenced the UNCITRAL Model Law. Both instruments contain rules which are similar, to a large extent. This section examines the rules of Article 4A, which regulates parties' liability for fraudulent EFT in US. Thus, to avoid repetition, this section examines Article 4A treatment of fraudulent EFT without demonstrating in every section the differences between the originator and the originator's bank liability for fraudulent EFT under Article 4A and in English agency law and contract law. Differences will be mentioned if they exist, in particular the "Statute of Repose" which exist under article 4A and does not exist under the UNCITRAL Model Law.

As with the UNCITRAL Model Law under Article 4A the originator and the originator's bank's liability for fraudulent EFT are determined according to the existence of two important factors. Firstly, the existence of agreement on security procedures should be used to authenticate the originator's payment orders. Secondly, whether the person who issues the payment order is one of the originator's employees, or one of the originator's bank's employees, or a third party. Furthermore, this section examines the originator's bank's liability for direct damages, consequential damages and interests under Article 4A. The purpose of the section is to demonstrate that the originator's rights and originator's bank's liabilities for damages and interests are predictable and certain, according to the "money- back

guarantee" rule and the exclusivity of Article 4A remedies. Therefore, this section demonstrates the exclusivity of Article 4A to determine the parties' liability for fraudulent EFT. Finally, section 505 "Statute of Repose"[80] of the Article 4A will be examined to demonstrate the originator's duty to notify the originator's bank of fraudulent EFT within limited time. The time limitation is very significant in determining the originator's right to refund the principal amount of funds transfer. Moreover, the time limitation makes the originator's bank's liability for fraudulent EFT certain unchangeable after a specific time, and protects the originator from unfair contract terms which limit the period of time to claim for a refund.

### 5.3.1 Unauthorised Payment Orders and the Parties' Agreement on the Security Procedures

The first step to be taken to determine the originator bank's liability for fraudulent payment order under Article 4A is to take into consideration whether an agreement on security procedures exists. [81] French argues that

> "[T]his threshold question [whether there is agreement on security procedures][82] is very important because its resolution, in most cases, will determine whether the bank or its customer bears the loss caused by the unauthorised payment order. If there was such an agreement, the customer will likely be bound to pay the order even if it was not authorised. If not, the receiving bank will likely be responsible for the unauthorised payment order."[83]

Under Article 4A, if there is no agreement on the security procedures to be employed to authenticate the originator's payment order, the originator bank's liability is

---

[80] The Official Comment to the U.C.C, note 2 supra, Comment on s. 4A -505.
[81] U.C.C section 4A-202, The Official Comment to the U.C.C ibid comment (1) on s. 4A- 203, Alvin C. Harrell, "UCC Article 4A," 2000, 25 Okla. City U.L.Rev.293 at p.301 and J. Kevin, French, " Unauthorized and erroneous payment orders," 1990, 45 Bus. Law. 1425 at p. 1426 and 1430.
[82] The words in square brackets added.
[83] French 1991, note 22 supra at p. 778.

determined under section 202(a) of Article 4A. [84] Under section 202 (a) of Article 4A, the originator's bank can debit the originator's account depending on only authorised payment order governed by the rules of agency law. [85] According to section 202 (a), the originator's bank is liable for fraudulent EFT issued, altered and amended by the fraudster, regardless of whether it is an authenticated payment order or not. [86] However, there are factors that the originator's bank can depend on to defend the liability under agency law, such as apparent authority or estoppel. [87] Given the distinctive nature of authenticating EFT, applying agency rules to electronic funds transfer leads to the uncertainty and unpredictability of the originator's bank and the originator's liability for fraudulent EFT. French states as follows:

> "[T]he fact that funds transfer payment orders are most often transmitted electronically inspired the drafters of Article 4A to look beyond the law of agency for loss-allocation formula. Applying the law of agency in all cases can have detrimental effects. Given the large sums typically moved by funds transfers, bank faced with the uncertainties of subsection 4A-202 (a) might be unwilling to accept payment orders unless they have assurance of authenticity. However, such absolute assurance cannot be obtained for electronic messages through the use of security procedures. As a result, the drafters were reluctant to apply to the law of agency to all funds transfer. The decision to formulate a different rule for cases in which a security procedure is used was based on the drafter's desire to preserve those aspects of funds transfers deemed most desirable in the pre-Article 4A system." [88]

French explains that since Section 202 (a) of Article 4A is devoted to paper based payment orders, applying it to electronic payment orders leads to uncertainty and unpredictability in the originator and the originator's bank's liability for fraudulent

---

[84] The Official Comment to the U.C.C, note 2 supra, comment (1) to the U.C.C section 4A- 203, French 1991, note 22 supra at p.778 and French 1990, note 81 supra at p. 1429.
[85] Thevenoz, note 11 supra at p. 935.
[86] ibid.
[87] ibid, The Official Comment to the U.C.C, note 2 supra, comment (1) to the U.C.C section 4A-203 and see Chapter two section 2.3.1 for more details on English Agency law and its effects on parties liability for fraudulent EFT.
[88] French 1991, note 22 supra at p. 781.

EFT. The drafters of Article 4A have designated section 202(b) of Article 4A to be applied to electronic payment orders, taking into consideration that most of the payment orders of large value funds transfer are transmitted electronically, not orally or in writing.[89] Under section 202(b), the originator's bank can debit the originator's account depending on authenticated payment order, according to the parties' agreement as to the security procedure whether the payment order is in fact authorised or not. [90] French [91] and Davis [92] rightly argue that section 202(b) of article 4A limits the originator's bank and the originator's liability for unauthorised electronic payment order. In a way, this should encourage the originator's bank to set up an agreement upon security procedures. French also argues that Article 4A provides the originator's bank and the originator "two paths of loss allocations" for fraudulent EFT as contained in section 202(a) and section 202(b). [93] Further, he persuasively argues that Article 4A motivates and encourages the originator's bank and the originator to agree on specific security procedures and be bound by section 202(b), for the following reasons.[94] Firstly, using security procedure reduces the chance that the bank will accept an unauthorised payment order issued in its customer name, which limits the bank's liability for unauthorised payment orders.[95] Secondly, according to the uncertain and unpredictable liability under section 202(a), the originator's bank might be reluctant to execute the customer's funds transfer unless there is an agreement to use security procedures. [96] Thirdly, where the originator's bank agrees to transfer the originator's funds without agreeing on security procedure, the bank

[89] ibid 781-782 and Thevenoz, note 11 supra at p.935.
[90] ibid.
[91] French 1991, ibid and Tony M Davis,, " Comparing Article 4A with Existing Case Law on Funds Transfers: A series of Case Studies," 42 Ala. L. Rev. 823, Winter 1991 at p.829.
[92] ibid.
[93] French 1991, ibid 782.
[94] ibid.
[95] ibid.
[96] ibid.

will increase the fee and reduce the speed to transfer money. This in turn affects the effectiveness of handling funds transfer. [97] Fourthly, the negotiation concerning security procedures between the originator's bank and the originator grants the originator the opportunity to choose the security procedure that he feels are efficient and comfortable for his business. [98] In *Tomaz Mendes Regatos* v *North Fork Bank and New Commercial Bank of New York*, [99] District Judge Scheindlind confirmed as follows:

> "[T]he drafters' aims are equally clear with respect to the unauthorized transfers of funds. They intended to encourage banks to implement security procedures for funds transfers. If no security procedure is in place, the customer has an absolute right to recover. If a security procedure *is* in place, and it is followed, the bank is absolved from loss. But if a security procedure is in place and the bank fails to follow it, that is as good as no security procedure at all: the loss reverts to the bank and the customer has an absolute right to recover. This allocation of loss is so integral to the structure of Article 4A that it may not be varied by contract." [100]

However, the originator's bank may be held liable for an authenticated but an unauthorised payment order, according to Section 203 (a) (1) and (2). [101] According to 203 (a) (1) the originator's bank and the originator may agree that the originator's bank is liable for an authenticated but unauthorised payment order, even if the requirements of section 202 (b) are met. [102] Such an agreement may allocate all the liability on the originator's bank for fraudulent EFT, or make the originator's bank and the originator agree to divide the losses.[103] While under Section 203 (a) (2) the originator's bank bears the liability for authenticated but unauthorised payment order even if the requirements of section 202(b) are met. The originator's bank liability for

---

[97] ibid 783-784.
[98] ibid 782-783.
[99] *Tomaz Mendes Regatos v North Fork Bank and New Commercial Bank of New York* 257 F. Supp.2d 632 (S.D. New York 2003)
[100] ibid 643.
[101] The Official Comment to the U.C.C, note 2 supra, comment (5) to the U.C.C section 4A-203 and Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.45.
[102] The Official Comment to the U.C.C, note 2 supra, comment (6) to the U.C.C section 4A-203.
[103] ibid.

such payment order where authenticated but unauthorised payment order is executed by one of the originator's bank's employee or a third party, will be examined subsequently in this chapter.

Moreover, under section 202(c) the originator's bank is entitled to debit the originator's account, depending on the payment order that is deemed to be authorised based on the security procedures chosen by the customer after the bank offered him and refused commercially reasonable security procedures. [104] Thevenoz demonstrates that the rationale behind Sections 202 (c) and 203 (a) 1 that drafters of Article 4A were not against "loss-spreading" [105] among the parties of EFT but they were concerned with "loss-avoidance." [106] The present author's view is that the originator's bank may offer to be liable for authenticated but unauthorised payment orders to compete with the other banks offer EFT services.

### 5.3.2 The Originator and the Origintor's Bank's Liability for Fraudulent EFT Executed by Variant Fraudsters

According to Section 202 of Article 4A, the originator and the originator's bank's liability for authenticated but an unauthorised payment order are determined according to the party who issued the unauthorised payment order. As mentioned earlier in this chapter the person who initiates unauthorised payment orders could be one of the originator's employees or one of the originator's bank's employees or a third party. The forthcoming pages examine the originator and the originator's bank's liability for fraudulent EFT, which are executed by the above-mentioned persons

[104] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.41.
[105] Thevenoz, note 11 supra at p.939.
[106] ibid.

under Article 4A. To demonstrate that the originator and the originator's bank's liability for fraudulent EFT are more predictable and certain.

**(a) The Parties' Liability for Fraudulent EFT Executed by the Originator's Employees**

Suppose in the hypothetical case mentioned previously in this chapter that the fraudster who issued the unauthorised electronic payment order is from the "customer shop," and the payment order is issued and transmitted electronically. Further, there is an agreement between the originator's bank and the originator on the security procedures according to section 202 (b) and (c). If the payment order is an authenticated payment order according to section 202 (b) and (c) and issued by one of the originator's employees, the originator's bank is not liable for fraudulent EFT and is entitled to debit the originator's account. [107] The originator can sue the fraudster (his employee) for the amount that is debited from his account as a result of fraudulent EFT. As mentioned earlier in this chapter, it is understandable why the originator should bear the liability for such payment orders, because the originator is in the best position to protect the transmitting device controlled by him and to choose reliable employees.[108]

Conversely, if the payment order is not an authenticated payment order according to section 202 (b) and (c) the originator's bank is liable for fraudulent EFT issued by one of the originator's employees. [109] Such cases happen if the originator's bank does not comply with section 202 (b) and (c)'s conditions. For example, when the bank acts in

[107] The Official Comment to the U.C.C, note 2 supra, comment (2) to the UCCC s. 4A-203.
[108] See Section 2.2.2, p.13.
[109] Thevenoz, note 11 supra at p.942.

bad faith, or when the bank does not employ commercially reasonable security procedures, or the originator bank employees does not verify the payment order in compliance with the security procedures.

In *Centre-Point Merchant Bank Ltd* v *American Express Bank Ltd,* [110] a fraudulent payment order for $702,976.63 was issued by a Centre-point employee who had access to a Centre-point telex room and telex machine. American Express bank found the payment order was an authenticated payment order according to security procedures agreed upon with Centre-point. [111] According to section 202(b) of Article 4A the District Court dismissed the plaintiff's claim based on the reasoning that the plaintiff's payment order was authenticated by the security procedure agreed on with the customer.[112] Therefore, the court found that the payment order was an authenticated payment order according to 202(b) of Article 4A, and accordingly, the originator's bank was not liable for the fraudulent payment order. [113] The present author's view that section 202 (b) and (c) gives the originator's bank the authority to debit the customer's account whether the authenticated payment order is in fact authorised or not. Consequently, French rightly argues the originator's bank's liability for such a payment order is predictable and certain and the originator's bank will not be reluctant to execute EFT at high speed and low-cost. [114] As well as being under the UNCITRAL Model law, the originator and the originator's bank's liability for authenticated but unauthorised payment orders under Article 4A are more predictable and certain than under English agency law and contract law. [115]

---

[110] *Centre-Point Merchant Bank Ltd* v *American Express Bank Ltd* WL 1772874 (S.D.N.Y 2000).
[111] ibid 4-6
[112] ibid.
[113] ibid.
[114] French 1991, note 22 supra, at p. 781-782.
[115] See section 5.2.2. of this chapter for more details.

**(b) The Parties' Liability for Fraudulent EFT Executed by the Originator's Banks' Employees and a Third Party.**

Fraudulent EFT might be executed by a person who is not one of the originator's employees, in particular, one of the originator's bank's employees or a third party. Since it is unfair that the originator bears the liability for authenticated but unauthorised payment orders executed by a third party and not facilitated by the originator's negligence. Section 203(a) (2) of Article 4A gives the originator the right to shift back the liability for an authenticated but unauthorised payment order to the originator's bank. According to section 203 (a) (2) of Article 4A the originator's bank is liable for fraudulent EFT whenever the customer proves that the payment order was issued by a person not in his company or a third party that does not obtain access to the information or the facilities from a source controlled by the customer. [116] Consequently, the originator's bank cannot debit the originator's account, according to fraudulent EFT executed by the originator's bank employees, or where a third party gains access to the information or facilities from the sources controlled by the bank[117] and any other sources not controlled by the customer. For example, when the originator's bank and the originator communicate through the Internet to execute EFT, and the fraudster intercepts the transmission of the payment order and alters the payment order. In such situation the originator's bank is not entitled to debit the originator's account provided that the interception by the fraudster was not facilitated by the originator's negligence or executed by using the sources controlled by the originator. According to section 203 (a) (2), if the fraudster obtains access to the

[116] French 1991, note 22 supra at p. 815 and Baker and Brandel, note 17 supra at p.13-34.
[117] The Official Comment to the U.C.C, note 2 supra, comment (5) to the U.C.C section 4A-203.

facilities and the information through the sources controlled by the customer, the customer is liable for fraudulent EFT "regardless of how the information was obtained or whether the customer was at fault." [118] This means that if the originator proves that he did not breach his duty of trust against the bank, the originator is still liable if fraudulent EFT occurs as a result of the originator's negligence. [119]

As mentioned previously in this chapter, enacting rules stipulate that the originator's bank is liable for authenticated but unauthorised payment orders issued by a third party, protect the originator from unfair contract terms. In such a contract, the originator's bank may include terms to exclude or limit its liability for fraudulent EFT executed by a third party.[120] Thevenoz provides a persuasive argument as to why the originator's bank should bear liability for such payment orders, as follows:

> "...since the losses caused by proven or persuasive outsiders are essentially determined by the bank's choice of technology and procedures of funds transfers, the banks are in the best position to account for them in the economic calculation and find the optimal trade-off between incremental costs and residual losses. They are also in the best position to spread those residual losses over all participants in funds transfer. Such provision could be varied by agreements among banks, but not with their customer." [121]

The present author's view is that according to Section 203 a (2), Article 4A imposes on the originator and the originator's bank a duty to keep and protect the sources and the transmitting facilities controlled by them from being accessed by an unauthorised person. [122] Otherwise one of the parties will be responsible for an authenticated but unauthorised payment order executed by a fraudster who obtains access through the sources controlled by him, which is either the originator or the originator's bank.

---

[118] Article 4A-203 (a) (2).
[119] Geva 1994, note 61 supra at p. 2-71 and Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p 45.
[120] ibid.
[121] Thevenoz, note 11 supra at p.947.
[122] Article 4A- 203(a)(2).

Consequently, the originator will not be liable for an authenticated but unauthorised payment order initiated by a third party who has obtained access to the sources not controlled by the originator. As indicated before, [123] under English agency law, the originator does not owe the originator's bank a duty to protect the sources he controls. The present author's view is that excusing the originator from such duty increases the possibility of fraudulent EFT occurring, because the originator would not be keen to protect his information and devices sources. This is also imposing the originator's bank to a massive liability for authenticated but unauthorised payment orders which makes the originator's bank reluctant to execute EFT at high-speed and low cost. As in the absence of such duty the originator's bank's liability for an authenticated but unauthorised payment order is unpredictable and uncertain. [124] Therefore, the present author's view that particular rules are needed to regulate the originator's duties towards the originator's bank and *vice-versa* in the context of EFT rather than the rules designed for other types of payment transactions. This would protect the originator from unfair contract terms and make the originator's bank's liability more predictable and certain.

[123] See section 2.2.2 of this chapter.
[124] ibid.

### 5.3.3 The Originator's Bank's Liability for Damages Against the Originator

As mentioned earlier in this chapter, the originator may suffer damages as a result of fraudulent EFT. Damages could be direct, such as losing the principal amount of money been transferred or consequential damages such as losing a preferable contract or losing the interests that would have been added to the originator's account if it were not debited. This section examines the originator's bank's liability for these damages, under Article 4A. To demonstrate that the originator's bank's liability under article 4A is more predictable and certain and the originator is entitled to a refund for the principal amount of the funds transfer and interests. The next section will demonstrate that the originator's bank liability for damages cannot be varied by parties' agreement in order to protect the originator from unfair contract terms which the bank include in its contract to exclude or limit its liability for an authenticated but unauthorised payment order.

#### (a) The Originator's Bank's Liability for Direct Damages and Interest

Under Article 4A, the originator's bank is under no duty to accept payment order unless it is contractually bound to accept the payment order by an express agreement[125] or according to a funds transfer system rules. [126] Accordingly, the originator's bank, which entered into an agreement with the originator to accept and execute the originator's payment order, may be held liable for breach of contract for executing fraudulent EFT that violates such an agreement. [127] Article 4A has

[125] Article 4A-212.
[126] ibid.
[127] Article 4A- 202, 203,204, 402(d).

regulated the originator's bank liability for damages and interests occurring as a result of fraudulent EFT, as based on the contractual relationship and Article 4A provisions.[128] However, there is reciprocal duty on the customer to notify the originator's bank in respect fraudulent EFT, otherwise the originator is not entitled to refund the principal amount or interest. [129] The time limitation and the originator's duty to notify the originator's bank in respect of fraudulent EFT will be examined in section 4 of this chapter. As such, limitation and duty affect the originator's right to claim a refund and the originator's bank's liability for fraudulent EFT. [130]

The originator's bank, if liable for fraudulent EFT, is obliged to refund the amount of the fraudulent payment order to the originator with interest, according to sections 204 and 402. If the originator's bank is held liable for a fraudulent EFT that is executed depending on unauthorised payment order under section 202 or unenforceable payment order under section 203, [131] the originator's bank must refund the amount of the payment order and interest on that amount according to section 204 (a) of Article 4A which states as follows:

> "[I]f a receiving bank accepts a payment order issued in the name of its customer as sender which is (i) not authorized and not effective as the order of the customer under Section 4A-202, or (ii) not enforceable, in whole or in part, against the customer under Section 4A-203, the bank shall refund any payment of the payment order received and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund...."

The originator's bank is liable to pay interest in respect of the fraudulent amount of money for the period, from the date the bank receives the payment or from the day the

---

[128] Article 4A-204, 402(d).
[129] ibid and Article 505.
[130] James J. White and Robert S. Summers, *Uniform Commercial Code* 3rd ed, West Publishing Co., St. Paul, Minn, 1993 at p. 207, 209.
[131] French 1991, note 22 supra at p. 818-819 and The Official Comment to the U.C.C, note 2 supra, comment (1) to the U.C.C section 4A-204.

originator's account debited to the day of refunding the money. [132] The rate of interest that should be paid could be ascertained by the parties agreement, otherwise it must be paid according to Federal Funds rate. [133]

According to section 402 (d) the originator's bank is obliged to refund any payment received from the originator for any payment order the originator was not obliged to pay for, plus interest. [134] Under Article 4A the "money- back guarantee rule" applies between a sender and its receiving bank, according to which the originator can seek refund from the originator's bank only.[135] Thus, the originator cannot "skip over" the originator's bank and seek refund from an intermediary bank, because there is no privity in the relationship between the originator and the intermediary bank. [136] The "money-back guarantee" rule requires privity in the relationship between the sender and the receiving bank to seek a refund from the receiving bank. [137] In *Grain Traders, INC v Citibank,* the Court of Appeals, second Circuit held as follows:

> "[I]n sum, we agree with the district court's thoughtful analysis and conclude that s 4-A-402 allows each sender of a payment order to seek refund only from the receiving bank it paid. Not only do the provisions of Article 4-A support the district court's interpretation, there are sound policy reasons for limiting the right to seek a refund to the sender who directly paid the receiving bank. One of Article 4-A's primary goals is to promote certainty and finality so that "the various parties to funds transfers [will] be able to predict risk with certainty, to insure against risk, to adjust operational and security procedures, and to price funds transfer services appropriately."... . To allow a party to, in effect, skip over the bank with which it dealt directly, and go to the next bank in the chain would result in uncertainty as to rights and liabilities, would create a risk of multiple or inconsistent liabilities, and would require intermediary banks to investigate the financial circumstances and various legal relations of the other parties to the transfer. These are matters as to which an intermediary bank ordinarily should not have to be concerned and, if it were otherwise, would impede the use of rapid electronic funds transfers in commerce by causing delays and driving up costs. Accordingly, we affirm the

---

[132] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.45.
[133] ibid at p.46 and Article 4A-506.
[134] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.60.
[135] *Grain Traders, INC v Citibank, N.A* 160 F.3d 97 (2nd Cir 1998) at p. 101.
[136] ibid 102.
[137] ibid 101, 102.

district court's dismissal of Grain Traders's refund claim under Section 402(4)." [138]

The present author agrees with the court's view allowing the customer to "skip over" the originator's bank seeking for refund affects Article 4A main policy to make the parties' duties, rights and liabilities for EFT predictable and certain.

Patrikis *et al* provide a convincing argument as to why the "money-back guarantee" rule providing the customer (originator or sender) with protection is not available under English agency law, for the following reasons. [139] Firstly, applying the agency law does not give the originator the protection to refund the money if the payment order is not completed. As long as the originator's agent (the originator's bank) acts reasonably in accomplishing the funds transfer, the originator's bank, under the rules of agency law, is not obliged to refund the money back. [140] The "money-back guarantee" rule confirms that under Article 4A the relationship between the originator and the originator's bank is not an agency relationship. [141] Consequently, the rules of agency law are not applied to the electronic funds transfer transactions in the context of Article 4A. [142]

Secondly, in England it is common for banks to limit or exclude their liability for fraudulent EFT. [143] On the contrary, under Article 4A, namely the originator's right to obtain a refund from the originator's bank under the "money-back guarantee" rule, this rule is mandatory and cannot be changed by the parties' agreement. [144] Lastly, in England, banks mostly in their standard terms contracts exclude liability for negligence of their intermediary banks that engage in to carry out the funds

---

[138] ibid 102.
[139] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.60.
[140] ibid.
[141] ibid.
[142] ibid 59.
[143] Azzouni, note 72 supra at p.361.
[144] Article 4A-402(f).

transfer.[145] According to such terms, the originator cannot sue the originator's bank to refund the money the fraudulent EFT has executed as a result of the intermediary bank's negligence. On the other hand the originator is not entitled to sue the intermediary bank, because there is no contractual relationship between them, or privity in contract. In such a case, the originator bears alone the liability for fraudulent EFT, which occurs as a result of the intermediary bank's negligence which is employed by the originator bank. Thus, the "money-back guarantee" rule protects the originator from such liability by stipulating strict liability on the originator's bank to refund the principal amount of the funds transfer to the originator.

However, the originator may instruct the originator's bank to route the funds transfer through a specific intermediary bank, and the originator's bank is obliged to follow the originator's instructions according to section 302(a) (1). Thus, if the intermediary bank, chosen by the originator, is held liable for fraudulent EFT and becomes unable to refund the money, because is not permitted by the applicable law or because the bank suspends payments.[146] In such a case, the originator is not entitled to obtain a refund from the originator's bank; therefore, the originator bears the risk of the intermediary bank failure to refund money and the originator's bank is entitled to payment from the originator. [147]

---

[145] J. Wadsly and A.G. Penn, *The Law Relating to Domestic Banking* 2nd ed, Sweet& Maxwell, London, 2000, at p. 375, Richard Hooley and John Taylor, "Payment by Funds Transfer," Michael Q.C. Brindle and Raymond Cox (eds) 3rd ed, *Law of Bank Payments*, Sweet& Maxwell, London, 2004, Section V. Recovery of Payments at p.126 and Xavier Thunis, "Recent Trends Affecting The Banks' Liability During Electronic Funds Transfer," J.I.B.L. 1991, 6 (8), 297-309 at p.229.

[146] Article 4A-402 (e) and The Official Comment to the U.C.C, note 2 supra, comment (2) to the U.C.C section 4A-402.

[147] ibid.

**(b) The Originator's Bank's Liability for Consequential Damages**

Under Article 4A, the originator's bank is not liable for consequential damages that may occur as a result of fraudulent EFT [148] unless there is an express written agreement between the originator and his bank which stipulates that the originator's bank is liable for consequential damages in case of the bank failure to execute the payment order. [149] Patrikis *et al* persuasively argue that Article 4A exempts the originator's bank from liability for consequential damages to fulfil the main goal of Article 4A, which is efficiency in executing EFT at high speed and low cost. [150] This can be justified by stipulating that the originator's bank should bear liability for consequential damages, making its liability uncertain and unpredictable. Patrikis *et al* explain that business transaction parties prefer to know beforehand their liabilities for failure to execute a duty to insure against that loss or to charge the required fees for potential loss. [151] Furthermore, if there is liability for consequential damages without requiring an express agreement, this may raise a debate as to which damages are foreseeable and which party in the best position to avoid loss. This makes the bank cautious and makes them implement preventive measures in executing EFT. Such measures hinder the swift execution of EFT. [152]

However, the originator's bank, in failing to execute the payment order, is liable for the expenses the sender pays in transaction, incidental expenses and interest losses. [153] Moreover, according to section 305(e) the originator's bank is liable for a "reasonable

[148] Article 4A-305(d) and Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.61.
[149] ibid.
[150] Patrikis, Baxter, Jr. and Bhala 1993, ibid at p.103.
[151] ibid at p.104
[152] ibid at p.105.
[153] ibid.

attorneys fees" where the originator demands recovery before bringing an action in the court and the originator's bank refuses to recover. [154]

However, the exclusivity of remedies under Article 4A only applies to actions for breach of Article 4A's provisions, but not to actions based on other grounds, for instance, common law or equity law. [155]In *Hedged Investment Partners v Norwest Bank* [156] the court held as follows:

> "[W]e analyze Article 4A's exclusivity differently. Drawing from the comments and the developing case law, we conclude that the exclusivity of Article 4A is restricted to situations that are covered by particular provisions of the Article and that principles of law and equity may be applied to disputes relating to funds transfers so long as those principles do not create rights, duties, or liabilities inconsistent with those stated in the Article." [157]

In other words, common and equity law apply in conjunction with Article 4A, so long as there is no inconsistency with Article 4A's provisions. [158]The exclusivity of Article 4A will be examined in the next section.

### 5.3.4 Exclusivity of Article 4A and Freedom of Contract

Article 4A regulates and governs the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. [159] Accordingly, the originator's basis for action against the originator's bank should be based on Article 4A provisions. The drafters of article 4A demonstrated that it is not appropriate to have recourse to principles of law or equity to determine rights, duties and liabilities inconsistent with

---

[154] Article 4A-305(e) and Patrikis, Baxter, Jr. and Bhala 1993, ibid.
[155] Harrell, note 80 supra at p.308 and Geva, Benjamin, " UCC Article 4A in the Courts: recent Developments", Nov/Dec 1998, 115 Banking L.J. 1016 at p. 1032.
[156] Hedged Investment Partners, L.P., et a.l v Norwest Bank Minnesota, N.A., 1998, 578 N.W.2d 756(Minn. App).
[157] ibid at p. 771.
[158] ibid.
[159] Ahn, Hyung J, " Note Article 4A of the Uniform Commercial Code: Dangers of Departing from a Rule of Exclusivity," 85 Va. L. Rev. 183, Feb 1999 at p. 183.

article 4A previsions. [160] The drafters of article 4A demonstrated as follows:

> "[I]n the drafting of Article 4A, a deliberate decision was made to write on clean slate and to treat a funds transfer as a unique method of payment to be governed by unique rules that address the particular issues raised by this method of payment. A deliberate decision was also made to use precise and detailed rules to assign responsibility, define behavioural norms, allocate risks and establish limits on liability, rather than to rely on broadly stated, flexible principles. In the drafting of these rules, a critical consideration was that the various parties to funds transfers need to be able to predict risk with certainty, to insure against risk, to adjust operational and security procedures, and to price funds transfer services appropriately. This consideration is particularly important given the very large amounts of money that are involved in funds transfers." [161]

In *Centre- point Merchant Bank Ltd v American Express Bank Ltd,*[162] the originator (Centre-Point) sued the originator's bank (American Express Bank) alleged common-law tort and contract claims, as well as claims under New York Uniform Commercial Code (UCC) arising out of bank transfer funds from investment account pursuant to fraudulent payment order. The originator alleged, *inter-alia,* that firstly, the originator's bank had breached the UCC provisions. Secondly, the originator bank was negligent for failing to provide a commercially reasonable security procedure. Thirdly, the originator alleged fraud and fraudulent concealment; negligent misrepresentation for that it had paid money for fraudulent payment order. Finally, Centre-Point alleged that all of these events amounted to a breach of duty of good faith and fair dealing. The American Express bank sought to dismiss all claims except the claim under the UCC, asserting that the dispute involves a wire transfer, and that UCC Article 4-A provides an exclusive remedy for such disputes. McKenna J. of United States District Court (New York) stated thus:

> "[W]hile Article 4-A should be the first place parties look for guidance when they seek to resolve claims arising out of a funds transfer, "the article has not completely eclipsed the applicability of common law in the area. The

[160] ibid at p.191-192 and The Official Comment to the U.C.C, note 2 supra, comment to the U.C.C section 4A-102.
[161] The Official Comment to the U.C.C, ibid.
[162] *Centre-Point Merchant Bank Ltd v American Express Bank Ltd* 913 F. Supp. 202 ( S.D.N.Y 1996).

> exclusivity of Article 4-A is deliberately restricted to 'any situation covered by particular provisions of the Article.' Conversely, situations not covered are not the exclusive province of the Article." In fact, the Official Comment tacitly states that resorting to principles of law or equity outside of Article 4-A is acceptable, so long as it does not create rights, duties and liabilities "inconsistent with those stated in this Article." [163]

Since sections 201 to 204 of Article 4A deal with the security procedures and verification of payment orders, and these sections determine the rights, duties and liabilities of the parties, [164] Mckenna J. dismissed the common- law claims brought against the originator's bank for fraudulent payment order. [165] Thus, common law claims are precluded where there are specific provisions in Article 4A covering specific situations. [166] *In Grain Traders, INC v CITIBANK, N.A,* [167] the originator of the EFT brought a suit against intermediary bank under the Uniform Commercial Code (UCC) and principles of common law, seeking a refund for an alleged uncompleted transfer. The Court of Appeals, Second Circuit affirmed the judgment of the District court of New York by dismissing Grain Traders claims under common law. The Court of Appeals held that "[W]e also hold that Grain Traders's common law claims are precluded because they seek to impose liability on Citibank that would be inconsistent with the provisions of Article 4-A." [168]

Further, the originator's bank, under Article 4A, is not an agent for any other party in

---

[163] ibid 206.
[164] ibid.
[165] ibid 208.
[166] ibid.
[167] *Grain Traders, INC v Citibank*, note 126 supra. The American courts have precluded common law claims when such claims would impose liability inconsistent with the rights and liabilities expressly created by Article 4A in the following cases; *Banco de la Provincia de Buenos Aires v. BayBank Boston N.A.*, 985 F.Supp. 364, 369-70 (S.D.N.Y.1997) (for conversion claim to stand, it cannot be inconsistent with Article 4-A); *Centre-Point Merchant Bank Ltd. v. American Express Bank Ltd.*, 913 F.Supp. 202, 206 (S.D.N.Y.1996) (exclusivity of Article 4-A is restricted to any situation covered by particular provisions of the Article and resort to common law must not be inconsistent); *Sheerbonnet, Ltd. v. American Express Bank, Ltd.*, 951 F.Supp. 403, 407-08 (S.D.N.Y.1995) (same); *see Cumis Ins. Soc., Inc. v. Citibank, N.A.*, 921 F.Supp. 1100, 1110 (S.D.N.Y.1996) (claim for conversion failed because bank's actions expressly authorized by Article 4-A); *Aleo International, Ltd. v. Citibank, N.A.*, 160 Misc.2d 950, 612 N.Y.S.2d 540, 541 (Sup.Ct.1994) (no claim for negligence unless conduct complained of was not in conformity with Article 4-A).
[168] *Grain Traders, INC v Citibank*, ibid 106.

the funds transfer, and the relationship between the originator and originator's bank is a contractual relationship, not an agency relationship. [169] Section 212 of Article 4A states as follows:

> "[A] receiving bank is not the agent of the sender or beneficiary of the payment order it accepts, or of any other party to the funds transfer, and the bank owes no duty to any party to the funds transfer except as provided in this Article or by express agreement."

Thus, the originator bank's duties, obligations and liabilities for payment orders arise as a result of acceptance of payment order or of agreement. [170] These duties, obligations and liabilities are determined according to Article 4A rules or to agreements; otherwise the originator's bank has no duty, obligations and liabilities to perform towards any party of the funds transfer. [171] In *Hedged Investment Partners* v *Norwest Bank Minnesota,* [172] the Court of Appeals of Minnesota held, *inter-alia,* that principles of exclusivity of Article 4A do not prevent consideration of the customer's actions based on contract. [173] Accordingly, under Article 4A the originator's actions against the originator's bank and *vice-versa*, for fraudulent EFT should be based on breach of contract and breach of Article 4A provisions.

Article 4A provides the same general rules and strategy of the UNCITRAL Model Law, with regard to the freedom of contract between the parties of the funds transfers.[174] Under section 501 of Article 4A, the parties are permitted to vary their rights and obligations by agreement, unless there are specific sections which provide

---

[169] Article 4A-212 and The Official Comment to the U.C.C, note 2 supra, Comment on section 4A-212.
[170] ibid.
[171] ibid.
[172] *Hedged Investment Partners, L.P., et al. v Norwest Bank Minnesota, N.A.* 578 N.W.2d 756(Minn. App 1998).
[173] ibid 755.
[174] The Official Comment to the U.C.C, note 2 supra, comment (1) to the U.C.C section 4A-501, French 1990, note 81 supra at p. 1440, Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p 128 and Thomas C. Baxter and Raj Bhala, "The Interrelationship of Article 4A with Other Law," 1990, 45 Bus. Law. 1485 at p. 1494.

that they may not be varied by agreement. [175] The variation could occur by individual agreement between two parties or more, or by the rules of funds transfer systems. [176] The rules of funds transfer systems regulate and govern the rights and obligations of the participants' banks in the system.[177] These rules can overrule provisions of Article 4A, except Article 4A provisions which provide that they may not be varied by agreement. [178] French explained that the rules of payment systems directly affect the participating banks of that system. [179] However, such rules may indirectly affect the rights of non-participants of payment systems, for instance, the originator or the beneficiary of funds transfer which was transferred through that payment system. [180] French has stated that:

> "[B]oth subsection (b) and the official comments, however, make it clear that funds transfer system rules directly affecting the rights of participating banks may indirectly affect the rights of non-participants such as the non-bank sender. While rules governing bank participants may indirectly affect non-bank users in other contexts, it seems unlikely that such rules would be permitted to alter the rights of non-bank participants under section 4A-202 and section 203. Comment 7 to section 4A-203, in fact, states that a funds transfer system rule cannot change the section 4A-202 rights of a customer that is not a participating bank." [181]

The official comment on Article 4A states the following example: "a rule purporting to define rights and obligations of non-participants in the system would not be effective to alter Article 4A rights because the rule is not within the definition of funds transfer system rule." [182]

---

[175] ibid.
[176] ibid.
[177] An example of payment systems, Fedwire, CHIPS and CHAPS, see Chapter one for more details about these payment systems.
[178] The Official Comment to the U.C.C, note 2 supra, comment (1) to the U.C.C section 4A-501, French 1990, note 81 supra at p. 1440, Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p 128 and Baxter and Bhala 1990, note 174 supra at p. 1494.
[179] French, ibid at p.1441-1442.
[180] The Official Comment (1) to the U.C.C section 4A-501, French, ibid, at p. 1440, Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p 128 and Baxter and Bhala 1990, note 174 supra at p. 1494.
[181] ibid.
[182] The Official Comment to the U.C.C, note 2 supra, comment (1) to the U.C.C section 4A-501.

In the context of fraudulent EFT, section 202 (f) of Article 4A provides as follows: " [E]xcept as provided in this section and in section 4A-203 (a) (1), rights and obligations arising under this section or section 4A-203 may not be varied by agreement." Consequently, the originator's bank and the originator's liability for fraudulent EFT, according to sections 202 and 203, cannot be altered or varied by the parties' agreement with the rules of payment systems. [183] According to Section 204 (b) of Article 4A, the "money-back guarantee" rule is a mandatory rule regulating the originator's bank's liability for direct damages and interests. For this reason, the originator's bank's liability for direct damages and interests occur as a result of fraudulent EFT cannot be varied by the parties' agreement. Furthermore, the rules of payment systems that may indirectly affect non-participants cannot vary or alter the originator's bank and the originator's liability for fraudulent EFT, according to sections 202 and 203 of Article 4A. [184]

To conclude, under Article 4A the originator's bank and the originator's liability for fraudulent EFT cannot be varied by agreement. This means that Article 4A imposes strict liability on both parties for fraudulent EFT. Accordingly, the originator and the originator's bank's liability for fraudulent EFT under Article 4A is predictable and certain. This stimulates banks to execute payment orders at high speed, low cost and effectively, so as to protect the originator from unfair terms that some bank stipulate in their contract, to exclude or limit liability for fraudulent EFT.

[183] The Official Comment to the U.C.C, note 2 supra, comment (1) to the U.C.C section 4A-501 and French 1990, note 81 supra at p. 1441
[184] ibid.

### 5.3.5 The Originator's Duty to Notify the Originator's Bank of Fraudulent EFT and the "Statute of Repose"[185]

Article 4A has treated the originator's bank liability for damages and interests under sections 204, 402. [186] However, there is a reciprocal duty on the part of the customer to notify the originator's bank in respect of fraudulent EFT, otherwise the originator is not entitled to refund the principal amount or interests. [187] Under Article 4A, the originator's duty to examine the bank statement and notify the bank of fraudulent EFT within limited time affects the originator's bank's liability for such transactions. If the originator does not inform the bank about authenticated but unauthorised payment order within limited time, the originator will not be able to refund the principal amount and interest. The time limitation and the originator's duty to notify the originator's bank in respect of fraudulent EFT are not recognised in the UNCITRAL Model and English law. This section examines the originator's duty to examine the bank statement and notify the bank of fraudulent EFT; otherwise the originator loses his right to claim for interests. Then, this section evaluates section 505 of Article 4A the "Statute of Repose," when the customer loses his right to refund the principal amount of funds transfers. Since, the "Statute of Repose" affects the originator's bank liability for fraudulent EFT. This section will examine whether the "Statute of Repose" can be changed by parties' agreement. It demonstrates that the originator's duty to inform the bank cannot be changed by parties' agreement. This makes the originator's bank's liability for authenticated but authorised payment order which the originator's bank was not informed about it, is certain and predictable after a specific time.

[185] The Official Comment to the U.C.C section 4A-505.
[186] Article 4A-204, 402 (c).
[187] ibid and Article 505.

**(a) The Originator's Duty to Examine the Bank Statement and Notify the Bank of Fraudulent EFT**

Under section 204 (a), the originator is obliged to notify the originator's bank within a limited time about any unauthorised payment order, otherwise the originator will not be entitled to claim interest. [188] The drafters of article 4A demonstrate that the aim of the loss of interest penalty is to motivate the originator to investigate and control its account. [189] The originator is obliged to fulfil two duties to be entitled to claim interest for unauthorised payment orders: first, the originator under a duty to "exercise ordinary care" to determine that the payment order is fraudulent payment order and he does not issue such payment order; [190] secondly, the customer must notify the bank within a "reasonable time" of not more than 90 days from the date the customer is notified that the payment order was accepted by the originator's bank or that the originator's account was debited. [191] However, this time may be varied by agreement between the parties. The time the parties agreed on must not be "manifestly unreasonable." [192] French asserts as follows:

> "[A]lthough subsection 4A-204 (a) states that customers have "a reasonable time not exceeding 90 days" within which to report unauthorized payment orders, the amount of time a court finds reasonable may vary greatly depending upon the facts of any given case. For this reason, it is prudent for customers to negotiate agreements with their receiving banks establishing the time period which is considered a reasonable time under subsection 4A-204(a). Customers should ensure that the agreed period allows adequate time to discover and report unauthorised payment orders." [193]

---

[188] French 1991, note 22 supra at 819 and Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.46.
[189] The Official Comment to the U.C.C, note 2 supra, comment (2) to the U.C.C section 4A-204.
[190] ibid.
[191] ibid.
[192] Howard Darmstadter, " Wired: Problems with Electronic Funds Transfer Agreements," 121 Banking L.J. 646 at p. 651.
[193] French 1991, note 22 supra at 819.

Article 4A and the official comment on Article 4A does not define what is considered to be a reasonable time, because a reasonable time depends on the facts of each case.[194] However, the official comment demonstrates

> " [I]f a payment order for $ 1,000,000 is wholly unauthorized, the customer should normally discover it in far less than 90 days. If a $ 1,000,000 payment order was authorised but the name of the beneficiary was fraudulently changed, a much longer period may be necessary to discover the fraud. But in any event, if the customer delays more than 90 days the customer duty has not been met." [195]

Moreover, the clarity and the amount of information available in the bank statement or notification, which it sends to the customer, may affect whether the time is reasonable or not.[196] However, the customer should keep in mind that the 90 days period is the maximum. Thus the customer who reports after 90 days has failed to meet his duty under section 204 (a) of Article 4A and is not entitled to claim for interest. In *Tomaz Mendes Regatos* v *North Fork Bank and New Commercial Bank of New York,* [197] Scheindlin J.of District Court of New York held that

> "...the customer is not entitled to interest from the bank on the amount to be refunded if the customer fails to exercise ordinary care to determine that the order was not authorized by the customer and to notify the bank of the relevant facts within a reasonable time not exceeding ninety days after the customer received notification from the bank that the order was accepted or that the customer's account was debited with respect to the order." [198]

Moreover, the originator is under a duty to "exercise ordinary care" to examine the bank statement or notification and notify the bank of any unauthorised payment order. "Ordinary care" is not defined under Article 4A, but Patrikis *et al* confirmed that "ordinary care" is "the sort of care that a reasonable customer in similar

---

[194] The Official Comment to the U.C.C, note 2 supra, comment (2) to the U.C.C section 4A-204.
[195] ibid.
[196] French 1990, note 80 supra at p. 1442.
[197] *Tomaz Mendes Regatos* v *North Fork Bank and New Commercial Bank of New York* 257 F. Supp.2d 632 (S.D. New York 2003).
[198] ibid 641.

circumstances would exercise." [199] They further argue that when the bank statement or notification to the customer is not satisfactorily detailed in order to give the customer the opportunity to suspect whether the payment order was unauthorised. The customer cannot discover if there is an unauthorised payment order from aggregate information, thereby fulfilling his duties by using "ordinary care" in examining the bank statement. [200] Furthermore, section 204 imposes on the originator a duty to notify the bank quickly and promptly about fraudulent EFT to make it easier for the bank to refund the money from the fraudster. [201] The penalty for the originator's failure to fulfil the former duties is that he or she loses the right to claim for interest, [202] without affecting his right to refund the principal amount of funds transfer. The originator's right to obtain a refund of the principal amount of money from the originator's bank cannot be varied by agreement. [203]

**(b) The "Statute of Repose"**

The originator might not be entitled to claim for refunding the principal amount of the payment order according to section 505 of Article 4A. This section is called the "Statute of Repose." Section 505 of Article 4A states as follows:

> "[I]f a receiving bank has received payment from its customer with respect to a payment order issued in the name of the customer as sender and accepted by the bank, and the customer received notification reasonably identifying the order, the customer is precluded from asserting that the bank is not entitled to retain the payment order unless the customer notifies the bank of the customer's objection to the payment within one year after the notification was received by the customer."

[199] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.46.
[200] ibid.
[201] The Official Comment to the U.C.C, note 2 supra, comment (2) to the U.C.C section 4A-204.
[202] ibid and Baker, and Brandel, note 17 supra at p. 13-37.
[203] Article4A- 204(b).

The present author's view is that this section imposes a duty on the originator to check the notifications or the bank statements he may receive from the originator's bank, to notify him about any unauthorised payment order. The originator's duty to notify the bank is significant, for the originator's bank and the originator for two reasons; firstly, the customer's delay in notifying the bank may prevent the bank from quick recourse against the wrongdoer, due to the wrongdoer's insolvency or disappearance. [204] Secondly, the delay in notification gives the wrongdoer the ability to continue to issue an unauthorised payment order on behalf of the customer. [205] Malaguti argues as follows:

> "[I]n this situation, when the bank has in good faith honoured several subsequent unauthorised orders, the client might be held liable for any order subsequent to the reception of the statement which could have avoided such further fraudulent orders through a timely notification by the client(4A-204). Although in principle the bank is still responsible for unauthorised orders in this situation, the client is in this way given the incentive to control constantly to verify his financial transactions, without bearing the full risk of orders diligently sent." [206]

On the contrary, under English case law and contract law, the customer does not owe his bank a duty to exercise reasonable care to inspect the bank statement to discover the forged cheques and to notify the bank in order to avoid future forgeries.[207] Under English case, law the customer is under such duty; if there is a term in the contract states and specifies in clear language, that the customer must inspect the bank statement and notify the bank of forged cheques. [208] By analogy, the same rule

---

[204] Geva, note 30 supra at p.393.
[205] ibid.
[206] Malaguti, note 13 supra at p.286.
[207] See Chapter four s. 4.3.1.
[208] *Tai Hing Mill Ltd.* v *Liu Chong Hing Bank Ltd.*and others [1986] A.C.80,at p. 109-110.

applies to the originator in EFT, he is not obliged to inspect the bank statement and notify the bank unless such a duty stipulated expressly in the contract. [209]

If the customer does not owe his bank such a duty, this leads to unpredictability and uncertainty in the parties' liability. Besides, the originator's bank will be reluctant to execute the payment order at high speed and low cost. This is because the originator's bank through the electronic authentication means cannot determine whether the person who sends the payment order is an authorised person or not. On the other hand, as the originator is not obliged to inspect the bank statement and notify the bank, this facilitates for the fraudster to carry on issuing unauthorised payment order. This increases the originator's banks vulnerability and liability for any unauthorised payment orders, and the originator's bank may not be able to recover the money due to the fraudster insolvency or disappearance.

To conclude, under section 505 of Article 4A the customer is obliged to object for fraudulent EFT within one year after he was received a notification "reasonably identifying" the payment order. [210] The consequence of the customer's failure to notify the originator bank of his rejection to the payment order within one year is the loss of the principal amount of the payment order. [211] The present author's view that originator's duty to notify bank within limited time and the consequences of his failure achieve important goals. On one hand it motivates the originator to check the bank statement thoroughly and regularly to inform the originator's bank about authenticated but unauthorised payment order, otherwise the originator will be liable for such payment order. On the other hand, it helps the bank to predict its liability for authenticated payment order and be assured that after specific time the bank will not

---

[209] Geva 200, note 30 at p.401 and See Richard Hooley and John Taylor, "Payment by Funds Transfer," Michael Q.C. Brindle and Raymond Cox (eds) *Law of Bank Payments* 3rd ed, Sweet& Maxwell, London, 2004, at p.133

[210] French 1991, note 22 supra at p. 820 and The Official Comment to the U.C.C, note 2 supra, comment on section 4A-505.

[211] ibid.

be liable for authenticated but unauthorised EFT. Therefore, Section 505 provides that the bank's notification must reasonably identify the payment order. The bank's notification must show clearly that the originator's account is debited according to a specific payment order, so the customer can determine whether he has issued that payment order or not.[212]

**(c) Variation of the "Statute of Repose" by the Parties' Agreement**

Under section 505 of Article 4A if the originator does not notify his bank of his objection within one year after he has received notification of the payment order. [213] The originator is precluded from objecting to his bank that a payment order is a fraudulent payment order. Banks in standard contracts tend to shorten the period of notification, in order to confine and shorten the period of their liability for fraudulent EFT. This is because if the customer does not notify his bank of his objection within this limited time, the originator cannot sue the bank for a refund for fraudulent EFT. Therefore, the question that arises is whether shortening the one-year period of notification is permitted under Article 4A. Particularly, section 505 of Article 4A does not stipulate explicitly that the one-year period cannot be varied by the parties' agreement. On the other hand section 501 of Article 4A states that unless it is provided in article 4A, the rights and obligations of a party to a funds transfer may be varied by agreement. In *Regatos v North Fork Bank* [214] the bank and the customer agreed to shorten the one-year period provided by Article 4A to 15 days, during this time the customer could object to unauthorised payment order. Regatos objected for

[212] Patrikis, Baxter, Jr. and Bhala 1993, note 29 supra at p.46.
[213] The Official Comment to the U.C.C, note 2 supra, comment to the U.C.C section 4A-505.
[214] *Tomaz Mendes Regatos v North Fork Bank and New Commercial Bank of New York*, 2003, 257 F. Supp.2d 632 (S.D. New York).

two unauthorised payment orders after 15 days of account statements were received, but North Bank refused to recredit the customer account and Regatos sued North Bank. Regatos argued, inter-alia, that the 15 days notice period was unenforceable. The bank contended that Regatos' failure to object to the wire transfers within 15 days of the issuance of the statements as required by the account agreement estopped him from asserting this claim.

The court held that the one-year period could not be shortened by agreement; nevertheless that nothing in section 505 stipulated explicitly that it may not be varied by agreement. [215] The court rightly justifies its decision based on that shortening the one-year period time affects "invariable right" of refund under section 204 the "money-back guarantee" rule and section 202, [216] and contradicts the main goals and policies of Article 4A. [217] The court stated that those sections 204 and 202 of Article 4A are explicitly provide that they cannot be varied by agreement. [218] The bank cannot vary by agreement its duty to refund an unauthorised payment order according to section 202 and section 204 and does not provide that the customer's failure to notify the bank prohibits him to be refunded. [219] The court stated that

> "[N]othing in the statute explicitly prohibits the one year notice provision from being varied by agreement. Read in isolation, a bank and its customer could agree that notification must be made within any period of time, including fifteen days. However, the one year notice provision strongly implicates the invariable right of refund provided by sections 4-A-202 and4-A-204. Those sections explicitly state that an agreement cannot vary the duty of a bank to refund a transfer that was executed in derogation of the bank's duty to follow agreed-upon security procedures. Surely, a very short notice period would effectively eviscerate the absolute duty created by sections 4-A-202 and 4-A-204. Similarly, section 4-A-204 explicitly states that a customer's failure to give notice will not disturb her right to refund, and that provision may not be varied by agreement." [220]

---

[215] *Regatos v North Fork Bank*, ibid at p.642.
[216] ibid.
[217] ibid 644.
[218] ibid.
[219] ibid.
[220] ibid 642.

Accordingly, the court held that the 15 days notice period stipulated in the account agreement was invalid as a matter of law. The court continued even if the parties were permitted to vary the one-year period, the 15 days period was unreasonable. [221] Indeed, the long period of notification is probably of benefit to the customer, as the customer needs time to discover unauthorized payment order and identify the fraudster. [222] In contrast, the short period time of notification is likely of benefit to the bank, because the possibility to identify the fraudster and refund the money increases. [223] Thus, the bank can recover the money as soon as possible before the fraudster disappears or becomes bankrupt. Turner argues

> "[T]he one-year period in section A4-505 is not a lengthy one per se. The rationale of a contractual requirement to report unauthorized transfers, however is that prompt reporting may allow to identify the perpetrator and possibly recover the funds. In that context, the one-year period is virtually meaningless." [224]

He suggested that a modification in section 505 of Article 4A should be made by permitting the parties to shorten the one-year period time and at the same time stipulates a minimum shortened period cannot be varied by agreement. [225] The present author does not agree with shortening the one-year period time, as shortening the period does not give the customer enough time to discover and identify the fraudulent payment orders and the fraudster. Besides, under Article 4A, the customer bears the risk for an authenticated but unauthorized payment order, unless he can prove that the fraudster is a third party. Therefore, it is not fair for the customer to bear the liability and does not give him enough time to inspect and notify his bank of

---

[221] ibid 644.
[222] Paul S. Turner, "Symposium is the UCC Dead, or Alive and Well? Practitioners' perspectives; the UCC Drafting Process and Six Questions about Article 4A: is there a Need for Revision to the Uniform Funds Transfers Law?" 28 Loy.L.A.L.Rev.351, 1994 at p. 359.
[223] ibid.
[224] ibid.
[225] ibid.

unauthorized EFT. Accordingly, the one-year period time is a reasonable time for the customer to notify the bank, in particular for the big and sophisticated corporations. As such corporations may issue huge number of EFT in large values in a very short time, with that big number of transactions probably corporations need time to inspect and examine their financial transactions to discover fraudulent EFT.

## 5.4. CONCLUSION

In conclusion, the UNCITRAL Model Law and Article 4A have developed and adopted rules to deal particularly with the originator's bank and the originator's liability for fraudulent EFT. [226] Thus, under the UNCITRAL Model Law and Article 4A an authenticated payment order is an authorised payment order whether it is in fact authorised or not. [227] Accordingly, the originator's bank is not liable for a fraudulent EFT is issued by an unauthorised person, as long as the payment order is authenticated by the security procedures agreed to between the parties. [228] However, under the UNCITRAL Model Law and Article 4A the originator is not liable for an authenticated but unauthorised payment order issued by the bank's employees or a third party that executed the payment order by intercepting the security procedures or gaining access through the bank sources.[229] Moreover, under the UNCITRAL Model Law and Article 4A the originator's bank's liability is certain, because the originator's bank is obliged to refund to the originator the principal amount of the fraudulent EFT plus interest. [230] Furthermore, the bank cannot limit or restrict such liability by agreement, as the "money-back guarantee" rule cannot be varied by the

[226] Article 4A- 202 (b) and (c) and the UNCITRAL Model Law art. 5 (2)
[227] ibid.
[228] ibid.
[229] Article 4A-section 203 (a) 2 and the UNCITRAL Model Law art. 5 (4).
[230] Article 4A-section 204 (a) and 402 and the UNCITRAL Model Law art. 14.

parties' agreement. [231] Besides, the UNCITRAL Model Law and Article 4A remedies are exclusive, therefore the originator's bank is not liable for the consequential damages of fraudulent EFT, unless there is an agreement. [232] However, Article 4A imposes on the originator a duty to examine the bank statement and notify the originator's bank within a limited period of time about unauthorised payment orders.[233] Otherwise, the originator is not entitled to refund the interest if he does not notify the bank within a reasonable time not exceeding ninety days. [234] Moreover, the originator is not entitled to a refund of the principal amount of fraudulent EFT if does not notify his bank about unauthorised payment order within one year. [235]

As Chapter four argued, under English law, rules of contract and agency law, the originator's bank and the originator's liability for fraudulent EFT is uncertain and unpredictable. Applying contract law, agency law and the case law apply to forged cheque are inappropriate in dealing with fraudulent EFT. The present author argues that the UK regulations and the EU Directive need to be amended by adding specific rules regulating and governing the originator and the originator's bank's liability for fraudulent EFT. Such rules should regulate the parties' liability for authenticated but unauthorised payment orders by taking into consideration the security procedures used to authenticate electronic payment orders. Furthermore, the parties' liability for direct damages, consequential damages and interests should be included in these rules. The rules should make the parties' liability for the above-mentioned damages predictable and certain and cannot be varied by parties' agreement to protect the weaker party (the originator) in the relationship. This can be achieved by enacting

[231] ibid.
[232] Article 4A-section 305 (d) and the UNCITRAL Model Law art. 18.
[233] Article 4A-section 204.
[234] ibid.
[235] Article 4A-section 505.

mandatory rule provides that the originator's bank is obliged to reaccredit originator's account for authenticated but unauthorised payment order. Furthermore, specific rules should impose duty on the originator to check the bank statement and notify the bank about unauthorised payment order within limited time, otherwise the originator losses his right to claim for a refund. Moreover, the remedies under the UK Regulations and the EU Directive should be exclusive and cannot be varied by parties' agreement in regard to direct and interest but can be varies in regard to consequential damages. The amendments of the UK Regulations and the EU Directive should take into consideration the rules of the UNCITRAL Model Law and article 4A which regulate the parties' rights, duties and liabilities for fraudulent EFT.

# CHAPTER SIX
# CONCLUSION

International wholesale EFT is an important method of payment used by business customers to discharge their financial obligations. This thesis has examined the scope of the originator and the originator's bank's rights, duties and liabilities for fraudulent international wholesale EFT in the three legal systems, these being the English, the EU and the American legal systems, as well as the UNCITRAL Model Law on International Credit Transfer 1992. This thesis has defined EFT as a payment order issued by the originator, using electronic means to authorise the originator's bank to transfer funds from the originator's account to the beneficiary's account. The funds transfer is carried out through the banking system by debiting the originator's account at the originator's bank and crediting the beneficiary's account at the beneficiary's bank.[1] A fraudulent EFT is a payment order issued by a person who was not authorised by the originator to issue such a payment order. This person could be one of the originator's employees or one of the originator's bank's employees, or a third party. [2] In EFT, once the payment order is authenticated, the originator's bank accepts the payment order and executes it by transferring funds from the originator's account to the beneficiary's account at the beneficiary's bank. [3] Due to the distinctive nature of the authentication of EFT, the originator's bank cannot determine whether the payment order is an authorised payment order or not. The originator's bank

[1] For more detail see Chapter one, section 1.2.
[2] ibid, section 1.2.4.(b)
[3] ibid, 1.2.5.

receives the payment order on its computer screen, but it is difficult to identify the person who sends the payment order. [4]

Despite there being clear, fundamental differences between the authentication of electronic payment order and paper-based payment orders, there is in fact no comprehensive body of law that exists in England to govern and regulate the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. [5] In the absence of any particular rules that apply to EFT, such transactions are regulated by applying the rules of agency law, contract law and by analogy with the rules applicable to forged cheque. [6] These rules do not provide the originator with the protection he needs from unfair contract terms, as applying such rules exposes him to liability for fraudulent EFT executed by a third party. [7] Moreover, under the above mentioned rules, the originator's bank's liability for fraudulent EFT is uncertain and unpredictable, and this may make the originator's bank reluctant to execute EFT at high speed, low cost and in an effective way.[8] This is because applying contract law, agency law and conducting an analogy with the rules governing forged cheques, gives rise to legal problems which need to be regulated by particular rules. These are the problem of identity authentication, the distinction between authorised and unauthorised payment orders and the scope of the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. [9]

---

[4] ibid.
[5] Mark Hapgood, QC, *Paget's Law of Banking* 12th ed, Butterworths, London 2002 at p. 330.
[6] ibid.
[7] For more detail see Chapter two, section 2.3.
[8] ibid.
[9] For more detail see Chapter one section 1.2.5.

## 6.1 The Problems of Identity Authentication in English Law and EU Law

There is a significant, influential relationship between identity authentication and the authorisation of electronic payment orders. [10] Chapter two [11] has demonstrated that the identity authentication of the person who sends the payment order is hard for the originator's bank to determine where it receives the payment order by electronic means. In EFT, the originator's bank uses security procedures to verify the electronic payment order. Once the payment order is verified by passing the security procedures the payment order is an authenticated payment order. [12] However, such security procedures cannot identify the person who sends the payment order, or establish whether he was in fact authorised to do so or not. [13] Applying the rules of agency law, contract law and the rules applying to forged cheques to an authenticated payment order leads to uncertainty and unpredictability. [14]

If the authenticated payment order is authorised, the originator's bank is entitled to debit the originator's account and transfer funds. Meanwhile, if the authenticated payment order was an unauthorised payment order, the originator's bank would not be entitled to debit the originator's account and the originator's bank would bear the liability for such a payment order. Such a payment order could be issued as a result of the originator's negligence, or by one of the originator's employees who was not authorised to do so, or by a third party. Since the originator's bank cannot determine whether the authenticated payment order is authorised or not, the originator's bank will be reluctant to use EFT at high speed, low cost and effectively, because of the uncertainty and unpredictability of the liability for authenticated payment orders. To

[10] For more detail see Chapter two, section 2.3.1.
[11] ibid.
[12] Hapgood, note 5 supra at p. 336.
[13] ibid.
[14] For more derail see Chapter two section 2.3.

avoid such liability for authenticated but unauthorised payment orders, the originator's bank includes in their contract terms that exclude or limit their liability for such payment order. [15] This exposes the originator to unfair contract terms, and makes him liable for an authenticated but unauthorised payment order issued by a third party. It is unfair for the originator to be liable for an authenticated but unauthorised payment order issued by a third party where the security procedure breaks down without the originator's negligence. Moreover, the security procedures used to authenticate the originator's payment order are chosen and employed by the originator's bank. [16] If security procedures are broken by a third party because they are not reasonable and without the originator's negligence, the originator's bank should be liable for an authenticated but unauthorised payment order, not the originator.

For this reason, the present author argues that applying the rules relevant to paper-based payment order, namely, contract law, agency law and the rules applying to forged cheques are neither appropriate, nor adequate in seeking to govern EFT. Indeed, applying these rules may lead to uncertainty and unpredictability in terms of the originator's bank' liability for fraudulent EFT, and does not provide the originator with the required level of protection for unfair contract terms. Hence, particular rules devoted to EFT are needed to determine when the electronic payment order is an authorised payment order or not. Such rules must take into consideration the distinctive nature of an authenticated electronic payment order, which is entirely different from authenticating a paper-based payment order. Particular rules devoted to EFT are needed to apportion liability for authenticated but unauthorised payment orders between the originator and the originator's bank. Since liabilities cannot exist

[15] Hapgood, note 5 supra at p.336.
[16] Benjamin Geva, *Bank Collections and Payment Transactions, Comparative Study of Legal Aspects*, Oxford, New York: Oxford University Press, 2001, at p.395.

without the existence of duties the rules devoted to EFT must provide the originator and the originator's bank with their rights and duties toward each other. The originator and the originator's bank duties and rights in the context of fraudulent EFT are not clear and determined, according to English case law, which leads to uncertainty and unpredictability as regards of both parties' liability.

A thorough examination of the provisions of the EU Directive and the UK Regulations demonstrated that they are limited in application, as they apply to funds transfers up to 50,000 Euro or its equivalent in another EEA. [17] Given that the UK regulations are an implementation of the EU Directive, they only apply to EFT executed between the EU Member states. [18] Equally important, the EU Directive and the UK Regulations do not comprehensively regulate the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT. [19] The EU Directive and UK regulations do not solve the problem of identity authentication and its effect on the parties' liability for an authenticated but unauthorised payment order. Moreover, neither legislation contains rules to determine when the payment order is an authenticated or an unauthenticated payment order. Furthermore, the EU Directive and UK regulations do not devote any rules to determining what standards of security procedures should be employed by the bank. Accordingly, in England there is no statutory definition of what constitutes security procedures in the context of EFT. Besides, there are no rules to determine their legal effect on the originator and the

[17] Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, OJ L 043, 14/02/1997 P.25 – 30, Article 1 and Cross-Border Credit Transfer Regulations 1999, 1999 No 1876, Reg 2 (1).
[18] UK Regulations, ibid, Reg 2 (1)
[19] For more detail on the UK Regulations and the EU Directive flows see Chapter two sections 2.4 and 2.5.

originator's bank's liability for authenticated but unauthorised payment orders in the context of EFT.

In England, there are two kinds of legislation that regulate the validity of security procedures used in electronic communication, regardless of the type of transactions they are used for. These are the Electronic Communications Act 2000 and the Electronic Signature Regulations 2002. This legislation implements the EU Electronic Signature Directive (EC1999/93).[20] It further sets out the legal framework for e-signature and the certification authority services. It provides for the fact that simple and advanced signatures are, in fact, admissible and valid in legal procedures.[21] However, applying this legislation to fraudulent EFT does not solve the problem of identity authentication and its effects on the parties' liability for authenticated but unauthorised payment orders. [22] Even the existence of the TTP does not solve the problem of identity authentication, because the TTP issues a digital certificate, which provides that a particular company owns specific public and private keys. [23] The TPP's function is to make the originator's bank able to determine whether the payment order was sent by the originator, but it does not determine if the person who sent the payment order was authorised or not. The customer's private key is an electronic file, which is vulnerable and could actually be copied by intercepting the

[20] The Electronic Signatures Directive 1999/93/EC on a Community framework for electronic signatures, OJ L13 p. 12, 19 January 2000 (hereafter EU Electronic Signature Directive), Justine Harrington, "U.K. and European Legislative Initiatives regulating Electronic Commerce", Michael Chissick and Alistair Kelman, *Electronic Commerce, Law and Practice* 3rd ed, Sweet & Maxwell, London, 2002 at p. 309 and J. Murray, "Public Key Infrastructure Digital Signatures and Systematic Risk", (JILT),Issue 1, 2003.
http://elj.warwick.ac.uk/jilt/03-1/murray.html

[21] The Electronic Signatures Directive 1999, Article 2 and Electronic Communications Act 2000, section 7.

[22] For more detail see Chapter two section 2.5.

[23] ibid, Robertson, note 81 supra at p.226 and "Authentication in an Electronic Banking Environment", Federal Financial Examination Council. August 8, 2001 at p.6.
http://www.ffiec.gov/pdf/pr080801.pdf
http://www.ffiec.gov (obtained 24/04/2004)

network or Internet. [24] Accordingly, the TTP does not solve the problem of the parties' liability for authenticated but unauthorised EFT, which arise as a result of the application of the rules of agency law on EFT. As a result of this the bank may include a term in the contract to exclude or limit its liability for an authenticated but unauthorised payment order. In such a case, the originator bears the whole liability for an authenticated but unauthorised payment order even if it is not the customer's fault or negligence, and even if the implemented security procedures are unreasonable.

The present author argues that the implication of the Electronic Communications Act 2000 and the Electronic Signature Regulations 2002 in the context of EFT leads, on the one hand, to the e-signature being admissible evidence in the context of EFT. On the other hand, though, the legal effect of electronic signatures on the originator and the originator's bank's liability for unauthorised payment orders is not determined and is, therefore, left to the court's discretion. In the absence of particular rules regulating the legal effect of an e-signature on the originator, and the originator's bank's liability for authenticated but unauthorised payment order, the parties' liability is still governed by rules of contract law and agency law. Accordingly, the court may use the originator's and the originator's bank's agreement to evaluate the effect of an e-signature. The banks, in these agreements, stipulate terms which exclude or limit their liability for authenticated but unauthorised payment orders issued by a third party. Consequently, the originator might be liable for authenticated but unauthorised payment orders where the originator's bank does not implement reasonable security procedures. On the other hand if the court applies the rules of agency law, this gives rise to the problem of identity authentication. Despite the existence of the Electronic

[24] ibid.

Communications Act 2000 and the Electronic Signature Regulations 2002, the originator and the originator's bank liability for authenticated but unauthorised payment order remain unpredictable and uncertain in England.

## 6.2 Identity Authentication under the UNCITRAL Model law and Article 4A

The UNCITRAL Model Law and Article 4A of the UCC devote particular rules to regulating the originator and the originator's bank rights, duties and liabilities for fraudulent EFT's.[25] These rules take into consideration the distinctive nature of authenticating electronic payment orders, as the problems of identity authentication make the originator bank unable to differentiate between authorised and unauthorised payment orders. Both sets of legislation stipulate that if the electronic payment order is an authenticated payment order, then the originator's bank is entitled to debit the originator's account, whether the payment order is in fact authorised or not.[26] The originator is bound by an authenticated payment order, regardless of whether it is authorised in fact or not, if the required conditions met. Firstly, the originator's bank is obliged to implement commercially reasonable security procedures, and the originator must agree to these security procedures. Secondly, the originator's bank should comply with the security procedures when authenticating the originator's payment order. [27] Article 4A stipulates a further condition, which is that the originator's bank should accept the originator's payment order in good faith. [28] If the originator's bank fails meet all the above mentioned conditions the originator's bank is not entitled to debit the originator's account. Furthermore, UNCITRAL Model Law

[25] The UNCITRAL Model Law on International Credit Transfers 1992, Articles 2 (a) and (i), 4,5, 14, 18 and the Uniform Commercial Code Article 4A, sections, 103, 202, 203, 204, 501, 505 and 506.
[26] UNCITRAL Model Law, Article 5 and the Article 4A, Section 202.
[27] UNCITRAL Model Law, ibid and Article 4A, ibid.
[28] Article 4A ibid.

and Article 4A forbid the originator and the originator's bank from agreeing to employ security procedures which are not "commercially reasonable." [29]

Under the UNCITRAL Model Law and Article 4A, the originator's bank's liability for an authenticated payment order is predictable and certain, whether it is authorised or not. This certainty and predictability encourages the originator's bank to execute EFT at high speed, low cost and efficiently, the significant features of EFT. The originator's liability for authenticated but unauthorised payment orders forces the bank to implement "commercially reasonable" security procedures and comply with them. Moreover, both forms of legislation protect the originator from unfair contract terms, whereby the originator's bank excludes or limits its liability for authenticated but unauthorised payment order. In situations when the security procedures employed by the originator's bank are not "commercially reasonable" both forms of legislation stipulate that the parties are not allowed to agree on security procedures that are not "commercially reasonable."

It is worth noting that what is commercially reasonable for one funds transfer transaction is not necessarily commercially reasonable for another as the circumstances differ from one transaction to another. This is all the more the case since reasonableness of security procedures differs according to the circumstances of every funds transfer transaction, and the evolution of technology. The UNCITRAL Model Law does not define or limit what could be considered a reasonable security procedure. It is for the court to use its discretion to evaluate the circumstances of each funds transfer transaction. However, the official comments on the UNCITRAL Model

[29] UNCITRAL Model Law, Article 5 and Article 4A ibid.

Law provides circumstances that the court should take into consideration, so as to determine the reasonableness of security procedures such as type, size and frequency of payment orders. [30] Under article 4A the reasonableness of security procedures is a matter of law taking into consideration different factors for example, the type, size and frequency of payment orders, besides the originator's instructions to his bank. Moreover, the court should take into consideration the standard of security procedures, which are mostly adopted within the banking industry. [31]

## 6.3 Scope of the Originator's and the Originator's Bank's Liabilities for Fraudulent EFT in English and EU Law

In England the rules applying to forged cheques are applied by analogy to fraudulent EFT, to determine the originator and the originator's bank liability for fraudulent EFT.[32] Further, under English agency law and contract law, the parties' liabilities for fraudulent EFT depend on the originator's bank's' "broad duty" to exercise reasonable care and skill carrying out the payment order. [33] Thus, the negligence and fault of the originator and the originator's bank may facilitate the execution of a fraudulent payment order by their employees or third party. The application of the parties' duty to exercise reasonable care and skill in EFT leads to unpredictability and uncertainty in the originator and the originator's bank's liability for fraudulent EFT. This is because the means of performing a duty of reasonable care and skill in the

---

[30] International Credit Transfer: Comments on the Draft Model Law on International Credit Transfer: Reports of the Secretary-General (A/CN.9/346), UNCITRAL yearbook, vol. XXII, 1991, p.52-102 at p.65 para 9. ( hereafter Report of the Secretary-General 991) http://www.uncitral.org/pdf/english/yearbooks/yb-1991-e/yb_1991_e.pdf (obtained on 12/12/2005).
[31] Article 4A, Section 202 (c).
[32] Richard Hooley and John Taylor, "Payment by Funds Transfer," Michael Q.C. Brindle and Raymond Cox (eds) 3rd ed, *Law of Bank Payments*, Sweet& Maxwell, London, 2004, p.109 and Geva, note 16 supra at p. 393-400.
[33] Geva, ibid p.397

context of forged cheques is different from the means by which the same duty is performed in the context of fraudulent EFT.

In terms of forged cheques, the customer is under a duty to exercise reasonable care and skill in drawing cheques so as not to facilitate forgery, [34] such as drawing and signing a blank cheque or leaving spaces near the amount give the opportunity to a fraudster to fill the cheque out with a fraudulent amount. In terms of EFT, the payment order is issued and signed electronically. This makes it the originator's duty to exercise reasonable skill and care in issuing and signing a payment order, which is different from drawing a blank cheque or leaving spaces for words or numbers to be added. Geva has demonstrated that in EFT, the originator's negligence and fault may take the form of not securing the important information or the access device from unauthorised access. Further, the originator could be negligent in choosing a very easy or obvious password or PIN code, for example, the customer's name or birthday. Equally importantly the originator may not notify the originator's bank promptly about the theft of the access device or about unauthorised payment orders after receiving notification from the bank of any funds transfer.[35] Accordingly, there is a significant, indeed essential difference between the originator's duty to exercise reasonable skill and care in initiating and signing a cheque and EFT.

This demonstrates that an application of the rules applicable to forged cheques, so as to determine the originator and the originator's banks liability for fraudulent EFT is not helpful and may indeed lead to unpredictability and uncertainty. This is because English case law imposes a narrow duty on the customer towards his bank to exercise

---

[34] J. Wadsly, and A.G. Penn, *The Law Relating to Domestic Banking* 2nded, Sweet& Maxwell, London, 2000, at p.241.

[35] Geva, note 16 supra at p.394.

reasonable care and skill in avoiding the possibility of drawing forged cheques. [36] Under English case law, the customer is found not to be under any duty to inspect his bank statement and notify the bank about forged cheque. [37] Moreover, it is held that the customer does not owe his bank a duty to exercise reasonable care in carrying on business, including selecting employees, so as to detect or prevent forgeries. [38] Further, it is held that the customer does not owe his bank a duty to exercise reasonable care to protect and secure cheques or corporate seals. [39] Discharging the originator from the above-mentioned duties in the context of EFT makes the originator's bank reluctant to execute his originator's instructions at high speed, low cost and efficiently. The absence of any particular rules applying to EFT to regulate the originator's duties towards his bank makes the bank include unfair contract terms which exclude or limit their liability for fraudulent EFT. Accordingly, the originator and the originator's bank relationship in the context of EFT should not be entirely left to being regulated by the implied and express terms of contract. On the one hand, applying the implied terms leads to uncertainty and unpredictability in terms of the originator's bank's liability for fraudulent EFT, which affects executing EFT at high speed, low cost and efficiently. On the other hand, applying express terms imposes on the originator to unfair contract terms and the originator will thus be liable for fraudulent EFT where his negligence or fault is not the reason behind executing fraudulent EFT. Therefore, the originator and the originator's bank's relationship should be regulated by particular rules devoted to EFT as distinct from the rules that apply to paper- based payment orders.

---

[36] *Young v Grote*, (1827), 4 Bing. 253, *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd. and others* [1986] A.C.80 and *London Joint Stock Bank, Limited v Macmillan and Arthur*,[1918] A.C.777.
[37] *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd. and others, ibid.*
[38] Geva, note 16 supra at p.399 and *London Joint Stock Bank, Limited* v *Macmillan and Arthur*, note 36 supra.
[39] *London Joint Stock Bank, Limited* v *Macmillan and Arthur,* ibid and Geva, ibid.

Drawing an analogy between the bank's duty to exercise reasonable care and skill in carrying out paper-based payment orders and electronic payment order leads to uncertainty and unpredictably in terms of the originator's bank liability for fraudulent EFT. In England, the originator's bank is under a duty to exercise reasonable skill and care in carrying out the customer's instructions in the context of EFT by analogy with the rules that apply to forged cheques. [40] Therefore, the originator's bank must adhere to the originator's instructions and adopt a reasonable interpretation of the customer's unclear and ambiguous instructions. [41] In an electronic payment order, the originator's bank is more concerned with the authentication payment order than the content of the payment order. However, according to English case law, if the customer proves that the originator's bank knew, or should have known that the payment order was ambiguous, the court may hold the originator's bank as being negligent and as having acted unreasonably if it did not ask for clarification from the originator, even though the payment order was an authenticated payment order. [42] Accordingly, the originator's bank's liability in regard to an authenticated and unauthorised payment order depends on the court's interpretation of whether the originator's bank executed its duty with reasonable skill and care. Moreover, under English case law, the originator's bank is under a duty to exercise reasonable care and skill not to facilitate fraud. [43] Thus, the originator's bank should refrain from executing an order if the originator's bank is "put on enquiry" and has reasonable grounds for believing that the order is an attempt to misappropriate customer's

[40] *Royal Products Ltd v Midland Bank Ltd,* [1981]2 Lloyd's Rep.194.
[41] ibid and *Midland Bank, Ltd.* v *Seymour,* [1955] 2 Lloyd's Report.147.
[42] *European Asian Bank A.G. v. Punjab and Sind Bank* [1983] 1 Lloyd's Rep.611
[43] *Barclays Bank Plc* v *Quincecare Ltd,* [1992] 4 All E.R. 363 at p. 376.

funds.[44] In an authorised but authenticated payment order, the originator's bank is not able to determine whether the person who sends the payment order is misappropriating the originator's money. In such a situation, it is for the court to decide whether the originator's bank has executed reasonable care and skill in carrying out the originator's payment order.

The originator's bank is liable for its employees and agents' negligence in facilitating the execution of a fraudulent EFT. Therefore, the originator's bank owes the originator a duty to exercise reasonable care and skill to employ a reliable intermediary bank, as under English law, the intermediary bank is the originator's bank's agent. [45] However, to avoid liability for fraudulent EFT executed as a result of the intermediary bank's negligence the originator's bank's terms exclude all liability for such a payment order. Under s.3 of the Unfair Contract Terms Act 1977 such an exclusion term might be found reasonable in the context of business customers. [46] Therefore, under English common law, the originator will be liable for fraudulent EFT executed without his fault or negligence unless he can prove that the originator's bank has breached its duty to exercise reasonable care or that the exclusion clause was unreasonable, neither of these factors are easily proved. [47]

Further, the originator's bank is under a duty to exercise reasonable care and skill in employing reasonable and effective security procedures to authenticate the originator's payment order. [48] Since the originator's bank is the supplier of the security procedures, it will be liable for the flaws in the security procedures. Under

---

[44] ibid.
[45] Wadsly and Penn, note 34 supra at p.374.
[46] Unfair Contract Terms Act 1977 section 3(1) and *Calico Printers' Association, Ltd.* v *Barclays Bank, Ltd* [1931] 39 LI.L.Rep.51
[47] Wadsly and Penn, note 34 supra at p.375 and Hooley and Taylor, note 32 supra at p. 175.
[48] Geva, note 16 supra at p. 397 and Hooley and Taylor, note 32 supra at p.125.

English case law, it is not predictable and certain whether the originator's bank would be entitled to debit the originator's account depending on authenticated but unauthorised with the employment of reasonable security procedures. It depends on the court's interpretation as to whether the originator or the originator's bank has breached its duty to exercise reasonable care and skill in initiating or carrying out the payment order. An important question may arise as to who bears the liability for an authenticated but unauthorised payment order. In cases where neither the originator nor the originator's bank are negligent. Moreover, which party bears the liability if both parties are negligent? There is no clear answer under the English case law, and using the parties' negligence as the test leads to uncertainty and unpredictability, as demonstrated in this thesis. Therefore the present author argues that the originator and the originator's bank's rights, duties and liabilities need to be regulated by particular rules different from the rules that apply to paper-based payment order.

If an originator's bank debits the originator's account on the strength of fraudulent EFT, the former breaches its contractual duty to the latter to adhere to the originator's payment order. Breach of contract triggers the originator's bank's liability for the loss the originator suffers as a result of any unauthorised debiting of his account. Such losses entail direct damages, consequential damages and interest loss. The recoverability of these damages is subject to the remoteness rule of *Hadley v. Baxendale*, [49] which divides the damages that can be recovered to two types. The first type is the damages that "arise naturally" as a result of breaching the contract. These damages are direct damages and loss interest. The second type is the damages which do not arise "naturally" as a result of breaching the contract. Such damages are called

[49] *Hadley v. Baxendale* (1854) 9 Exch 341.

consequential damages. [50] According to the remoteness rules of *Hedley v. Baxendale* the damages arising naturally are recoverable while the damages that do not arise naturally are not recoverable unless such damages are in both parties' contemplation when they entered the contract. [51] In England, the courts' decisions were different in regards to the when the defendant's liability for consequential damages is triggered. In one decision, the court held that liability is triggered if the defendant was aware of the special circumstances that caused the claimant's losses. [52] Meanwhile, in other cases the court held that it was not enough that the claimant drew the defendant's attention to the special circumstance. He should have gone further to establish that the defendant accepted the liability of consequential damages. [53] EFT is used to discharge commercial transactions, which means that the originator's banks are aware that the originator uses EFT for commercial purposes. However, such awareness is not considered to be awareness of the special circumstances that the originator will suffer commercial losses. Moreover, it is not certain which type of damages could be classified, as they arise naturally as a result of unauthorised funds transfer. In an EFT transaction, the originator's loss could be much greater than the amount of funds transfer not executed properly. This includes losing a particularly profitable contract or losing the opportunity to tender for a contract. The unpredictability and uncertainty of the originator's liability for consequential damages makes the originator's bank reluctant to execute EFT at high speed, low cost and effectively.

---

[50] ibid.
[51] ibid, Harvey McGregor, *McGregoer on Damages* 17th ed, Sweet & Maxwell, London, 2003, at p.187 and Ewan Mckendrick, *Contract Law* 5th ed, Palgrave Macmillan, Basingstoke, 2003, p.424.
[52] *Simpson v. London and North Western Railway CO* (1876) 1 QBD 274 and *Seven Seas Properties Ltd v. AL-Essa* (No.2) [1993] 1 WLR 1083).
[53] *Horne v. Midland Railway*(1872-1873) L.R. 8 C.P. 131.

Mostly, the originator's bank in its standard terms contracts excludes or limits its liability for fraudulent EFT not executed by one of its employees. [54] Moreover, the originator's bank excludes and limits its liability for fraudulent EFT executed as a result of an intermediary banks' negligence. [55] In both situations the originator is not able to recover either the direct or consequential damages from the originator's bank, and is unable to recover them from any intermediary bank, as there is no privity in contract between them. The absence of particular rules regulating the originator's bank's liability for direct and consequential damages leads to unwanted results. Either there is unpredictability and uncertainty in the originator's bank liability where there is no express agreement to exclude its liability or the originator, as the weaker party, will bear the liability for fraudulent EFT not executed as a result of his negligence or fault, where the originator's bank explicitly excludes its liability for fraudulent EFT. Therefore, particular rules regulating EFT are needed to strike a balance between predictability and the certainty of the originator's bank's liability for fraudulent EFT and to protect the originator from unfair contract terms imposed by the originator's bank. This also leads to unpredictability and uncertainty as regards the originator's liability.

As indicated before, UK regulations are an implementation of the EU Directive, the applicable legislation is not a comprehensive legal framework. It is limited in its pecuniary limits, as it applies to credit transfers of up to 50.000 Euros. The UK Regulations and the EU Directive do not regulate the originator and the originator's

---

[54] Xavier Thunis, "Recent Trends Affecting The Banks' Liability During Electronic Funds Transfer," J.I.B.L. 1991, 6 (8), 297-309 at p.229 and Ahmed Azzoni, "Internet banking and the Law: a critical examination of the Legal controls over Internet banking in the UK and their ability to frame, Regulate and secure banking on the net," J.I.B.L.R. 2003, 18(9), 351-362 at p.361.

[55] Thunis, ibid, Wadsly and Penn, note 34 supra at p. 375 and Hooley and Taylor, note 32 supra at p.126 .

bank's rights, duties and liabilities for fraudulent EFT. The UK Regulations and the EU Directive do not stipulate when an electronic payment order is authorised or deemed to be authorised. [56] Moreover, the legislation does not provide for which party should be liable for an authenticated but unauthorised payment order executed by one of the originator's employees, or by one of the originator's bank's employee or by a third party. Accordingly, in England, the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT are still unpredictable and uncertain. The UK Regulations and the EU Directive do not impose a duty on the originator's bank to employ reasonable and effective security procedures. Moreover, the UK Regulations and the EU Directive provide that the "money –back guarantee" is applied to refund claims up 12.500 Euros. [57] Thus, if the originator suffers any loss of more than 12.500 Euros he can recover these losses according to contract law and tort law, but not according to the UK regulations or EU Directive. This causes more confusion for both the originator and the originator's bank as their liabilities will be regulated by different sources of law, namely the UK regulations and English agency and contract common law. The absence of a comprehensive framework governs the parties' rights, duties and liabilities for fraudulent EFT and the existence of different sources, and instead leads to unpredictability, uncertainty and unfair treatment for both parties.

[56] Anu Arora, " Round up: Banking Law," Comp. Law. 2000, 21(8), 234-244, at p. 244.
[57] The EU Directive, Article 8, UK Regulations, regulation 9 and Richard Hooley "EU Cross-Border Credit Transfers- the New Regime," B.J.I.B. & F.L.1999, 14(9), 387-395 at p. 393.

## 6.4 The UNCITRAL Model Law and Article 4A Treatment of Originator and the Originator's Bank's Liability for Fraudulent EFT

The present author argues that under the UNCITRAL Model Law and Article 4A of UCC, the originator and the originator's bank's liabilities for fraudulent EFT are more predictable and certain. Besides, the originator is protected from unfair contract terms that could be imposed by the originator's bank. Both legislation allocate the originator and the originator's bank's liability for authenticated but unauthorised payment order according to two significant factors, that is the parties' agreement on what commercially reasonable security procedures should be employed to authenticate the originator's payment order, and the fraudster who issues the payment order. [58] Under the UNCITRAL Model Law and Article 4A the originator's bank is entitled to debit the originator's account owing to authenticated payment order regardless of whether it is authorised or not. [59] However, the originator's bank is obliged to agree with the originator on the "commercially reasonable" security procedures that should be employed to authenticate the originator's payment order to be entitled to debit the originator's account. If there is no agreement between the originator and the originator's bank as to the security procedures, the originator's bank is not entitled to debit the originator's account depending on an authenticated but unauthorised payment order. In such a situation, the originator's bank bears liability for an authenticated but unauthorised payment order. According to the rules of agency law even the payment order is an electronic payment order, and may be authenticated by reasonable security procedures. [60]

---

[58] UNCITRAL Model Law, Article 5 and Article 4A, Sections 202 and 203.
[59] UNCITRAL Model Law, ibid and Article 4A, Section 202.
[60] UNCITRAL Model Law, ibid and Article 4A ibid

However, under UCITRAL Model Law and Article 4A, the originator can shift back to the originator's bank the liability for an authenticated but unauthorised payment order, even if it was authenticated by security procedures agreed on between them in two circumstances: when the authenticated but unauthorised payment order is executed by one of the originator's bank employees, or when it executed by a third party who did not gain access through the originator sources. [61] Under the UNCITRAL Model Law and Article 4A the above two conditions should be met to entitle the originator's bank to debit the originator's account. These conditions protect the originator against unfair contract terms the bank includes to exclude or limit their liability for fraudulent EFT executed without the originator's negligence or fault. Moreover, the originator's bank's liability for authenticated but unauthorised payment order is more predictable and certain as long as it agrees on the "commercially reasonable" security procedures with the originator. This would encourage the originator's bank to employ the most advanced and sophisticated security procedures to disclaim liability for authenticated but unauthorised payment orders.

In contrast to English agency law, under the UNCITRAL Model Law and Article 4A, the originator owes his bank a duty to keep and protect the sources and the transmitting facilities controlled by him from being accessed by unauthorised person. Thus the originator's bank will not be liable for authenticated but unauthorised payment order is issued by a third party who gained access through the sources controlled by the originator. Accordingly, the originator's bank will not be reluctant to execute EFT at high speed, low cost and in an effective way. This is because the originator's bank can predict its liability for a payment order is authenticated by

[61] UNCITRAL Model Law, ibid and Article 4A ibid

"commercially reasonable" security procedure and executed by a third party which does not gain access through the sources controlled by the bank. Under the UNCITRAL Model Law and Article 4A the originator and the originator's bank's liability for fraudulent EFT authenticated by security procedures agreed to, and executed by one of the originator's employees or one of the originator's bank's employees or third party cannot be varied by parties' agreement.[62]

Further, under the UNCITRAL Model Law and Article 4A, the originator's banks liability for direct and consequential damages is more predictable and certain than under English common law. This is because according to the "money-back guarantee" rules, the originator's bank is obliged to refund the principal amount of the fraudulent payment order, plus interest. [63] This is a mandatory obligation, and cannot be varied by the parties' agreement, which is again a protection for the originator from unfair contract terms that exclude or limit the originator's bank's liability for fraudulent EFT. [64] Further, under the UNCITRAL Model Law and Article 4A the originator's bank is not liable for the consequential damages the originator may suffer as a result of fraudulent EFT unless there is an agreement as to such liability. [65]

However, under Article 4A the originator is under a duty to "exercise ordinary care" to examine the bank statement and notify the originator's bank about any unauthorised payment order within a limited time. Otherwise, the originator is not entitled to refund the interest if he does not notify the bank within a reasonable time

[62] UNCITRAL Model Law, ibid and Article 4A, ibid.
[63] UNCITRAL Model Law, Article 14 and Article 4A, section 204.
[64] UNCITRAL Model Law, ibid and Article 4A, ibid.
[65] UNCITRAL Model Law Article 18 and Article 4A, section 305 (d).

not exceeding 90 days. [66] Further, the originator is not entitled to a refund of the principal amount of fraudulent EFT if he does not inform his bank about unauthorised payment order within one year. [67] Under English case law, the originator does not owe his bank a duty to exercise reasonable care and skill to inspect statements and to discover unauthorised payment orders and notify the originator's bank unless such duty is stipulated expressly in the contract. [68] The existence of such a duty assures the originator's bank that after a specific time, the bank will not be liable for authenticated but unauthorised payment orders. Moreover, the originator's duty to notify the originator's bank makes both of them aware that there is unlawful access to sources controlled by one of them or the security procedures employed by the bank are not effective and successful in protecting their communications. Once they are aware of unlawful access, they will undertake the required procedures to protect the sources controlled by them and stop fraudster from executing unauthorised in the future. Under Article 4A the parties are not allowed to shorten the one-year period time, as shortening it affects the "invariable right" of refund under the "money-back guarantee" rule and contradicts the main goals of Article 4A.[69] Given that corporations may issue a huge number of funds transfers within short time, they need time to examine the bank statement to discover fraudulent EFT.

---

[66] Article 4A, section 204.
[67] Article 4A, section 505.
[68] *Tai Hing Mill Ltd. v Liu Chong Hing Bank Ltd. and others*, not 36 supra.
[69] *Tomaz Mendes Regatos v North Fork Bank and New Commercial Bank of New York*, 2003, 257 F. Supp.2d 632 (S.D. New York).

## 6.5 The Way Forward

An examination of the current law as it applies to EFT in England has demonstrated that the current law is not appropriate and adequate to solve the problems that arise in the context fraudulent EFT. This is because the rules that apply to paper-based funds transfer are inappropriate in dealing with the distinctive nature of authenticating electronic payment order. Applying such rules gives rise to the following problems. Firstly, the problem of identity authentication and the appropriate criteria for the method to be applied to achieve this. Secondly, the legal value and the standards of security procedures which should be implemented to authenticate the originator's payment order. Thirdly, the allocation of loss, between the parties for authenticated but unauthorised EFT. Fourthly, the scope of the originator's bank's liability for direct damages and consequential damages occurred as a result of fraudulent EFT. Fifthly, the examination of the current law proves that currently under English common law the originator and the originator's bank's rights, duties and liabilities for fraudulent EFT is unpredictable and uncertain. Sixthly, there are no rules to protect the originator from any unfair contract terms that the originator's bank includes to limit or exclude its liability for fraudulent EFT. A thorough examination of the EU Directive on Cross-Border Credit Transfer and the UK Cross-Border Credit Transfer Regulations shows that both pieces of legislation are insufficiently comprehensive as they do not regulate the originator and the originator's bank's rights, duties and liabilities for International fraudulent wholesale EFT. Moreover, the EU Directive and the UK Regulations are limited in application as they applied to EFT up 50.000Euros and to EFT executed between Member States. As the EU Directive is a guide for the Member States to take into consideration when they enact their national law. Some EU Member States when,

they implemented the EU Directive in their domestic law have extended the limit of application of their domestic law beyond the Directive's ambit. [70] For instance, Denmark extended its legislation to cover countries out of the Member States and the EEA if these countries have equivalent rules. [71] Furthermore, Germany has extended the application of its domestic legislation to cover payment orders up to 75,000 Euro.[72] Some Member States such as Finland, Germany and Portugal apply the EU Directive to national credit transfers in addition to international credit transfers. [73] These examples show that the EU Directive lays down a minimum standard and that the Member States could apply its provisions more extensively in their domestic law. Accordingly, UK could have gone further in their application of the EU Directive by covering wholesale EFT without pecuniary or geographical limits.

Since applying the rules of English common law to international fraudulent wholesale EFT give rise to the legal problems mentioned earlier in this section the present author argues there is a need for new form of regulatory framework containing rules to regulate EFT other than the rules that apply to paper-based funds transfer. The regulatory framework must regulate and govern the following issues. First, the identity authentication of the person who sends the payment order, as it is difficult by electronic means alone to determine whether the person who sends the payment order is authorised to do so or not. Therefore, the rules enacted to regulate EFT should take into consideration the distinctive nature of the process of authenticating EFT and its

[70] Report from the Commission to the European Parliament and to the Council: On the Application of Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, Brussels, 29.11.2002, COM (2002) 663 final, at p. 10.
[71] Report from the Commission to the European Parliament and to the Council: On the Application of Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, Brussels, 29.11.2002, COM (2002) 663 final, at p. 10.
[72] ibid.
[73] ibid.

effects on the parties' liabilities for fraudulent EFT. Second, the rules must demonstrate, in light of the distinctive nature of authenticating EFT, when the payment order is an authorised payment order or not. Third, the rules should regulate the allocation of loss arising as a result of fraudulent EFT. In regards to the loss allocation the originator's bank should be liable for an authenticated but unauthorised payment order when it is executed by third part without originator's negligence or fault, even if it is not the originator's bank's fault if the security procedure implemented to authenticate the originator's payment order was chosen and implemented by the originator's bank. Meanwhile, where the authenticated but unauthorised payment order is issued as a result of the originator's negligence and fault, the originator should bear the liability for such a payment order. Fourth, the originator and the originator's bank rights, duties and liabilities in the context of EFT need to be regulated to be more predictable and certain. In regard to the originator's bank, the originator's bank should be under a duty to protect the important and essential information and access device controlled by it from unlawful access. In regards to the originator, the rules should impose a duty on the originator to protect the essential information and access devices controlled by him from unlawful access. Moreover, the originator should be under a duty to examine the bank statement and notify the originator's bank about unauthorised payment order within limited time, otherwise he will not be entitled to refund the principal amount or the interest. Five, the rules must impose duty on the originator's bank to employ reasonable and effective security procedures agreed on with the originator to authenticate the originator's instructions. The originator's bank should comply with security procedures when authenticating the originator's instruction, failure to comply should meant that the originator's bank bears the liability for the authorised payment order.

Six, equally importantly, the originator's bank's liability for direct damages, sequential damages and interest should be predictable and certain in advance, as is the case with the "money-back guarantee" rules under the UNCITRAL Model Law and Article 4A. Seven, it is important to include mandatory rules which provide that the loss allocation of fraudulent EFT and the originator's bank's liability for direct damages and interest cannot be changed by parties' agreement to protect the originator from unfair contract terms. Finally, since the advanced communication technology has promoted the number and the size of international EFT. Such rules should cover international wholesale EFT without pecuniary or geographical limits.

The provisions of the UNCITRAL Model Law and article 4A could be taken into consideration when enacting rules to regulate wholesale EFT as guides. Both legislation deal with and regulate the above-mentioned issues by devoting rules regulate EFT. These rules take into consideration the distinctive nature of EFT authentication.

**BIBLIOGRAPHY**

**BOOKS**


Akdeniz, Yaman, Walker, Clive and Wall, David (eds), *The Internet Law and Society*, Longman, Harlow, 2000.

Andoh, Benjamin and Marsh, Stephen, *Civil Remedies*, Dartmouth, Aldershot, 1997.

Anning, Paul, Ried, Emily and Rowe, Heather (eds), E-*Finance: Law and Regulation,* LexisNexis, London, 2003.

Arora, Anu, *Cases and Materials in Banking Law*, London, Pitman, 1993.

Arora, Anu, *Electronic Banking and the Law,* 2nd ed, IBC Business Publishing, London, 1995.

Arora, Anu, *Electronic Banking and the Law,* 3rd ed, IBC Business Publishing, London, 1997.

Baker, Donald I and Brandel, Roland E, *The Law of Electronic Fund Transfer Systems: Legal and Strategic Planning,* revised edition, Warren, Gorham & Lamont, Boston, 1996.

Basedow, Jurgen and Kono, Toshiyuki (eds), *Legal Aspects of Globalization,* 1st ed, Kluwer Law International, Cambridge, 2000.

Beale, H.G, Bishop, W.D & Furmston, M.P, *Contract Cases & Materials,* 4th ed, Butterworths, London, 2000.

Beatson, Jack, *Anson's Law of Contract,* 28th ed, OUP, Oxford, 2002.

Blair, William, *Banks and Remedies,* 2nd ed, Lloyd's of London Press, London, 1999.

Blair, William, *Banks Liability and Risk,* 3rd ed, Lloyd's of London Press, London, 2001.

Brindle, Michael Q.C. and Cox, Raymond Q.C (eds), *Law of Bank Payments*, 2nd ed, Sweet& Maxwell, London, 1999.

Brindle, Michael Q.C. and Cox, Raymond Q.C (eds), *Law of Bank Payments*, 3rd ed, Sweet& Maxwell, London, 2004.

Burrows, Andrew, *Remedies for Torts and Breach of Contract,* 2nd ed, Butterworths, London, 1994.

Chissick, Michael and Kelman, Alistair, *Electronic Commerce, Law and Practice,* 3rd ed, Sweet & Maxwell, London, 2002.

Clarkson, C.M.V & Hill, Jonathan, *Jaffey on The Conflict of Laws,* 2nd ed, Butterworths, London, 2002.

Cranston, Ross, *European Banking law: The Banker-Customer Relationship,* Lloyd's of London, London, 1993.

Cranston, Ross, *Principles Of Banking Law,* 2nd ed, OUP, Oxford, 2002.

Dassesse, Marc, Isaacs, Stuart and Penn, Graham, *EC Banking Law,* 2nd ed, Lloyd's of London Press, London, 1994.

Donnelly, Mary, *The Law of Banks and Credit Institutions*, Sweet and Maxwell, London, 2000.

Edwards, Lilian & Charlotte, Waelde, *Law & the Internet: A Framework for Electronic Commerce,* 2nd ed, Hart Publishing, Oxford, 2000.

Effros, Robert C. (ed), *Payment Systems of the World*, Oceana Publications, New York, London, 1996.

Ellinger, E, Lomnicka, Eva and Hooley, Richard, *Modern Banking Law,* 3rd ed, Oxford University Press, New York, 2002.

Ellinger, E, Lomnicka, Eva and Hooley, Richard, *Ellinger's Modern Banking Law,* 4th ed, oxford University Press, New York, 2005.

Geva, Benjamin, *The Law of Electronic Funds Transfers; Global and Domestic Wire Transfers, ACH payments, Consumer Transactions*, Mathew Bender, New York, 1994.

Geva, Benjamin, *Bank Collections and Payment Transactions, Comparative Study of Legal Aspects*, OUP, Oxford, 2001.

Goff & Jones, *The Law of Restitution,* 6th ed, Sweet & Maxwell, London, 2002.

Goldspink, Robert, and Cole, Jermey, *International Commercial Fraud,* 1st ed, Sweet and Maxwell, 2002.

Goode, Royston Miles, *Payment Obligations in Commercial and Financial Transaction*, Sweet & Maxwell, Centre for Commercial Law Studies, London, 1983.

Goode, Royston (ed), *Electronic Banking: The Legal Implications,* Institute of Bankers, London, 1985.

Goode, Royston Miles, *Commercial Law,* 2nd ed, London, Penguin, 1995.

Goode, Royston Miles, *Commercial Law,* 3rd ed, London, Penguin, 2004.

Hadding, Walther and Schneider, Uwe H. (eds), *Legal Issues in International Credit Transfers,* Duncker & Humblot, Berlin, 1993.

Hall, Maximilian, *Banking Regulation and supervision: A Comparative Study of the UK, USA and Japan*, Edward Elgar, Aldershot, 1993.

Hall, Maximilian, *Handbook of Banking Regulation and Supervision in the United Kingdom,* 3rd ed, Edward Elgar, Cheltenham, 1999.

Hapgood QC, Mark, *Paget's law of Banking,* 12th ed, Butterworths, London 2002.

Hapgood QC, Mark, *Paget's law of Banking,* 13th ed, Butterworths, London 2007.

Harris, Donald, Campbell, David and Halson, Roger, *Remedies in Contract & Tort,* 2nd ed, Butterworths, London, 2002.

Holden, Milnes, *The Law and Practice of Banking*, Vol.1, Banker and Customer, 5th ed, Pitman, London, 1991.

Horn, Norbert, *Legal Issues in Electronic Banking*, Kluwer Law International, London, 2002.

Harris, Donald, Campbell, David and Halson, Roger, *Remedies in Contract & Tort,* 2nd ed, Butterworths, London, 2002.

Kelleher, Denis and Murray, Karen, *IT Law in the European Union*, Sweet & Maxwell, London, 1999.

Kwaw, Edmund M.A, *The Law & Practice of Offshore Banking & Finance*, Quorum Books, London, 1996.

Laidlaw, Andrew and Roberts, Graham, *Law Relating to Banking Services,* 2nd ed, the Chartered Institute of Bankers, London, 1992.

Levi, Michael, *Regulating Fraud: White-collar Crime and the Criminal Process*, Tavistock Publications, London, 1987.

Lodder, Arno R. and Kaspersen, Henrik W.K., *E Directives: Guide to European Union Law on E-Commerce: Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection*, Kluwer Law International, Netherlands, 2002.

Malaguti, Maria Chiara, *The Payment System in the European Union Law and Practice*, Sweet& Maxwell, London, 1997.

Markesinis, B.S. and Munday, R.J.C. *An outline of the Law of Agency,* 3rd ed, Butterworths, London, 1992.

Mckendrick, Ewan, *Contract Law,* 5th ed, Palgrave Macmillan, Basingstoke, 2003.

McGregor, Harvey, *McGregoer on Damages,* 16th ed, Sweet & Maxwell, London, 1997.

McGregor, Harvey, *McGregoer on Damages,* 17th ed, Sweet & Maxwell, London, 2003.

Mitchell, Jeremy, *Electronic Banking and the Consumer, the European Dimension*, Policy Studies Institute, London, 1988.

Munir, Abu Bakar, *Internet Banking: Law and Practice*, LexisNexis, London, 2004.

Norton, Joseph (ed), *Banks Fraud and Crime*, Published Jointly with The Centre For Commercial Law Studies, Lloyd's of London Press, London, 1994.

Norton, Joseph (ed), *Banks Fraud and Crime*, 2nd ed Published Jointly with The Centre For Commercial Law Studies, Lloyd's of London Press, London, 2000.

Norton, Joseph, Reed, Chris and Walden, Ian (eds), *Cross-Border Electronic Banking, Challenges and Opportunities*, Published Jointly with The Centre For Commercial Law Studies, Lloyd's of London Press, London, 1995.

Ogus, Anthony I., *The Law of Damages*, Butterworths, London, 1973.

O'Mahony, Donal, Peirce, Micheal and Tewari, Hitesh, *Electronic Payment systems for E-Commerce,* 2nd ed, London, 2001.

Patrikis, Ernest T, Baxter, Thomas C, Jr. and Bhala, Raj K, *Wire Transfers: A Guide to U.S. and International Laws Governing Funds Transfers*, Irwin, Illinois, 1993.

Penn, G.A, Shea, A.M and Arora, A., *Banking Law: The Law and Practice of International Banking*, Vol.2, Sweet& Maxwell, London, 1987.

Pennington, R.R, Hudson, A.H and Mann, J.E, *Commercial Banking Law*, Macdonald and Evans, Plymouth, 1978.

Reed, Chris, *Electronic Finance Law*, Woodhead-Faulkner, Cambridge, 1991.

Reed, Chris, *Legal Regulation of Internet Banking A European Perspective*, Centre for Commercial Law Studies, London, 1996.

Reed, Chris, Walden, Ian and Edgar, Laura (eds), *Cross-Border Electronic Banking, Challenges and Opportunities,* 2nd ed, Published Jointly with The Centre For Commercial Law Studies, Lloyd's of London Press, London, 2000.

Reynolds, F.M.B and Graziadei, Michele, *Bowstead and Reynolds on Agency,* 17th ed, Sweet & Maxwell, London, 2001.

Reynolds, F.M.B and Graziadei, Michele, *Bowstead and Reynolds on Agency,* 18th ed, Sweet & Maxwell, London, 2006.

Revell, Jack, *Banking and Electronic Fund Transfers*, OECD, Paris,1983.

Roberts, Graham, *Law Relating to Financial Services,* 5th ed, The Chartered Institute of Bakers, Canterbury, 2003

Rose, Francis D. (ed), *Restitution and Banking Law*, Mansfield Press, Oxford, 1998.

Scot, Hal and Wellons, Philip, *International Finance, Transactions, Policy and Regulation,* 6th ed, New York, Foundation Press, 1999.

Scot, Hal and Wellons, Philip, *International Finance, Transactions, Policy and Regulation,* 7th ed, New York, Foundation Press, 2000.

Scot, Hal and Wellons, Philip, *International Finance, Transactions, Policy and Regulation,* 9th ed, New York, Foundation Press, 2002.

Smith, Graham J.H and Others, *Internet Law and Regulation,* 3rd ed, Sweet& Maxwell, London, 2002.

Smith, Roy and Walter, Ingo, *Global Banking,* New York, Oxford University Press, 1997.

Tunkel, Daniel and York, Stephen (eds), *E-Commerce A Guide to the law of Electronic Business,* 2nd ed, Butterworths, London, 2000.

Ulph, Janet, *Commercial Fraud: Civil Liability, Human Rights, and Money Laundering,* Oxford University Press, 2006.

Wadsly, J. and Penn, A.G., *The Law Relating to Domestic Banking,* 2nd ed, Sweet& Maxwell, London, 2000.

Welch, Brain (ed), *Electronic Banking and Treasury Security,* 2nd ed, Woodhead, Cambridge, 1999.

Wheeler, Mike and Oldfield, Roger, *International Insolvency Procedures,* 2nd ed, Blackstone Press, London, 1997.

White, James J. and Summers, Robert S, *Uniform Commercial Code,* 3rd ed, West Publishing Co., St. Paul, Minn, 1993.

White, James J. and Summers, Robert S, *Uniform Commercial Code,* 5th ed, West Group, St. Paul, Minn, 2000.

Ziegel, Jacob S. (ed), *New Developments in International Commercial and Consumer Law:* Proceedings of the 8th Biennial Conference of the International Academy of Commercial and Consumer Law, Hart, Oxford, 1998.

Zilioli, Chiara and Selmayr, Martin, *The Law of the European Central Bank*, Hart Publishing, Oxford, 2001.

## ARTICLES

Ahn, Hyung J, " Note Article 4A of the Uniform Commercial Code: Dangers of Departing from a Rule of Exclusivity," 85 Va. L. Rev. 183, Feb 1999.

Angel, J. "Why Use Digital Signatures for Electronic Commerce?" Commentary (JILT), Issue 2,1999.
http://elj.warwick.ac.uk/jilt/99-2/angel.html (obtained on 27/04/2004).

Arora, Anu, " The Jack Committee Report on Banking Services: Law and Practice," Comp.Law.1991, 12(7),127.

Arora, Anu, "Contractual and Tortious Liability in EFT in the United Kingdom," L.C & A.I. 1992,1(3), 291.

Arora, Anu, " Round up: Banking Law," Comp. Law. 2000, 21(8), 234.

Arora, Anu, "Unfair Contract Terms in International Banking Contracts," J.B.L. 2001, Sep, 553.

Azzouni, Ahmed, "Internet banking and the Law: a critical examination of the Legal controls over Internet banking in the UK and their ability to frame, Regulate and secure banking on the net," J.I.B.L.R. 2003, 18(9), 351.

Baxter, Thomas C. and Bhala, Jr. Raj, "The Interrelationship of Article 4A with Other Law," 1990, 45 Bus. Law. 1485.

Bergsten, Eric E, "UNCITRAL Model Law on International Credit Transfer," J.I.B.L. 1991, 6(7), 276.

Bhala, Raj, " International Payments and Five Foundations of Wire Transfer Law," Essays in International Financial & Economic Law No, 2, International Finance and Tax Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, University of London, in cooperation with the London Centre for International Banking Studies and the London Institute of International Banking, Finance and Development Law, London, 1996.

Bohm, Nicholas, Brown, Ian and Gladman, Brian, "Electronic Commerce: Who Carries the Risk of Fraud?" (JILT) Issue 3,2000.
http://elj.warwick.ac.uk/jilt/00-3/bohm.html (obtained on 27/04/2004).

Bojer, Lotte, "International Credit Transfers: The Proposed EC Directive Compared With The UNCITRAL Model Law," J.I.B.L. 1995, 10 (6), 223.

Brandon, George, " What you Should Know about Wire-Transfer Liabilities," Financial Executive, Nov-Dec 1990 v6 n6 p39(5).

Campbell, Andrew and Cartwright, Peter, "Bank Insolvency Issues," Insolvency L.J. 2002, 6(Oct), 198.

Brazell, Lorna, "Electronic Security: Encryption in the Real World, E.I.P.R.1999, 21(1),17.

Brookes, Victoria and Murray, Rodger G, "Cross-Border Credit transfers: Legislative Comment," I.B.F.L. 1997, 15(11), 128.

Cheng, Charles L.A, " The UNCITRAL Model Law on International Credit Funds Transfers," Sing. J. Legal Studies. 538, Dec, 1993.

Coats, Sam and Morgan Joe, "Victims of Internet Bank Fraud Will have to Pay up," The Times, November, 13, 2004.

Coleman, Claire, "Electronic Signatures in Banking," F & C.L.2001, 3(5),1.

Dale, Richard, " Controlling Risks in Large Value Interbank Payment Systems," J.I.B.L. 1997,12(11), 426.

Dale, Richard, " Reforming Japan's Payment, Clearing and Settlement Systems: Part 1: Large Value Interbank Payment Systems," J.I.B.L. 1999, 14(6), 177.

Darmstadter, Howard, " Wired: Problems with Electronic Funds Transfer Agreements," 121 Banking L.J. 646.

Dassesse, Marc, "Cross-Border Payments: A Need to Reassess Priorities," J.I.B.L. 1993, 8 (5), 169.

Datt, Sunil, "Regional and Global Developments in Electronic Funds Transfer and Cross-Border Payments," North American Journal of Economics & Finance, 1996, Vol 7, issue 2, p. 191.

Dawson, Simon, "Computer Fraud: Part 1: The Risk to Business," C.T.L.R.1999, 5 (3), 70.

Davis, Tony M, " Comparing Article 4A with Existing Case Law on Funds Transfers: A series of Case Studies," 42 Ala. L. Rev. 823, Winter 1991.

Di Brozolo, Luca G. Radicati, " International Payments and Conflicts of Laws," 48 Am.J. Comp. L. 307, Spring 2000.

Donnelly, Mary, "Electronic Funds Transfers: Obligations and Liabilities of Participating Institutions," C. L. Pract.2003, 10 (2), 35.

Effros, Robert C, "A Banker's Primer on the Law of Electronic Funds Transfers," 105 Banking L.J.510 Nov-Dec 1988.

Effros, Robert C, "Legal Issues in Payment Systems Reform," Journal of International Banking Regulation, 1999, Vol/Part 1, 193.

Ellineger, E, "The Giro System and Electronic Transfers of Funds," L.M.C.L.Q. 1986, 2 (May), 178.

Felsenfeld, Carl, " Strange Bedfellows for Electronic Funds Transfers: Proposed Article 4A of the Uniform Commercial Code and the UNCITRAL Model Law," 42 Ala. L. Rev. 723, Winter 1991.

Felsenfeld, Carl, The Compatibility of the UNCITRAL Model Law on International Credit Transfers with Article 4A the UCC, Fordham Law Review, 1992, May, 53.

Fisher, Jonathan, "Bank and Customer Relations: Fraud," J.I.B.L. 1986. 1(1), 47.

Ford, M, "Identity Authentication and 'E-Commerce," (JILT), Issue 3,1998. http://elj.warwick.ac.uk/jilt/98-3/ford.html(obtained on 27/04/2004).

French, J. Kevin, " Unauthorized and erroneous payment orders," 1990, 45 Bus. Law. 1425.

French, J. Kevin, " Article 4A's treatment of Fraudulent Payment Orders-the Customer's Perspective," 1991, 42 Ala. L. Rev.773.

Fry, Patricia B, " Basic Concepts in Article 4A: Scope and Definitions," 45 Bus. Law. 1401, June 1990.

Geva, Benjamin, " Payment into Bank Account," J.I.B.L.1990, 5(3), 108.

Geva, Benjamin, " Allocation of forged Cheque Losses-Comparative Aspects, Polices and a Model for Reform," L.Q.R.1998,114 (4), 250.

Geva, Benjamin, " UCC Article 4A in the Courts: recent Developments", Nov/Dec 1998, 115 Banking L.J. 1016.

Gill, Mark, "Responsibility and Electronic Funds Transfer," I.B.F.L. 1994, 13 (7), 4.

Gillies, Lorna, "A Review of the New Jurisdiction Rules for Electronic Consumer Contracts within the European Union," Commentary, (JILT), Issue 1, 2001. http://elj.warwick.ac.uk/jilt/01-1/gillies.html (obtained on 27/04/2004).

Gkoutzinis, Apostolos, "Cross-border electronic banking activities in the single European market and the normative value of home country supervision," Journal of International Banking Regulation, Vol 5,No.1, 2003, p.78.

Harrell, Alvin C, "UCC Article 4A," 2000, 25 Okla. City U.L.Rev.293.

Hartley, Trover, "Interim Measures Under The Brussels Jurisdiction and Judgements Convention," E.L.Rev, 1999, 25(2), 178.

Hamzah, Zaid, "Technology Risk Management in Internet Banking: developing a Structured and Proactive Legal Protection Regime," Ad. Bus. 2003, 2.1(15).

Heller, Stephanie, "The New CHIPS: Intraday Finality—Revolutionary or Evolutionary?" Banking & Finance Law Review, June 2003, 18 BFLR-CAN 395.

Hooley, Richard, "EU Cross-Border Credit Transfers- the New Regime," B.J.I.B.& F.L.1999, 14(9), 387.

Huertas, Thomas F, " Payment Systems in Europe," E.F.S.L. 1995, 2(8), 220.

Jack, Robert, " Still Waiting for Legislation," Scottish Banker, 1994.

Johnson, Adam, "Jurisdiction and Choice of Law in Claims for Restitution: Some Lessons for Bankers and Banking Lawyers," J.I.B.L. 1999, 14 (8), 253.

Johnson, Clare, "Electronic Banking: Some Legal Issues," I.B.F.L.1994, 13(7),1.

Kariyawasam, Rohan, "Internet Interconnection: Where are we Going," C.T.L.R. 2000,6(7), 187.

Kolodziej, Andrzej, "Customer-Banker Liability in Electronic Banking," Comp. Law. 1986, 7(5), 191.

Kyles, Dianna, " The Concept of Payment: Wire Transfer Orders, The Common Law and Article 4A," Dalhousie Journal of Legal Studies, 2002, 217.

Lamond, A and Davis, R.H, "Electronic Funds Transfer in UK Banking System," International Journal of Information Management, 1991, June, Vol 11, Issue 2,105.

Lockett, Nick, "How to Secure Electronic Transactions," I.F.L.Rev.1999, 18(3), 9-11.
Mason, Stephen,"E-Banking and Authentication," Amicus Curiae, 2002, 41(May/June), 22.

Maduegbuna, Samuel O. "The Effects of Electronic Banking Techniques on the Use of Paper-Based Payment Mechanism in International Trade," J.B.L.1994, Jul, 388.

Malaguti, Maria C, " Legal Issues in Connection with Electronic Transfers of Funds," L.C. & A.I. 1992, 1(3), 275.

Mason, Stephen, "Electronic Signatures in the EU and World E-Commerce: Technical and Legal Ramifications," Computer and Law, Dec 1999/Jan 2000, Vol.10,Issue 5, 37-44. http://www.itsecurity.com/papers/digsig.htm( obtained on 24/07/2004).

Mason, Stephen, "E-Banking and Authentication," Amicus Curiae Issue 41 May/June 2002.

Maysami, Ramin Cooper and Mills, Kim, "Regulation and Supervision of Online Banking Services in the United States: an Integrated Approach," J.I.B.L.R. 2004, 19 (11), 447.

McCullagh A et al, "Signature Stripping: A Digital Dilemma," Refereed article, (JILT), Issue1, 2001.
http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html (obtained on 27/04/2004).

McKelvy, Tina E, "Article 4A of the Uniform Commercial Code: Finally, Banks and their Customers Know Where they Stand and Who Pays When a Wire Transfer Goes Awry," 21 Mem. St.U. L. Rev. 351, Winter, 1991.

Murray, J," Public Key Infrastructure Digital Signatures and Systematic Risk," (JILT),Issue1,2003.
http://elj.warwick.ac.uk/jilt/03-1/murray.html (obtained on 27/04/2004).

North, Peter, "Private International Law: Change or Decay?" (2001) 50, 3, I.C.L.Q, 477-508.

Ormerod, David, "The Fraud Act 2006-Criminalising Lying," legislative Comment, Crim. L.R. 2007, Mar, 193-219

Radcliffe, Nicola, "Towards Uniformity in the Rules Governing Electronic Funds Transfers," B.J.I.B. & F.L. 1988, 3(3), 364.

Reed, Chris, "What is a Signature?" (JILT), Issue 3, 2000.
http://elj.warwick.ac.uk/jilt/00-3/reed.html/ (obtained on 27/04/2004).

Rendon, David,"The formal regulatory approach to banking regulation," Journal of International Banking Regulation," Vol 2,No.4, 2001, p.27.

Sappideen, Razeen, "Cross-Border Electronic Funds Transfers Through Large Value Transfers Systems and The Persistence of Risk," 2003, J.B.L., p.584.

Sappideen, Razeen, "The regulation of credit, market and operational risk management under the Basel Accord," 2004, J.B.L.p.59.

Schu, Reinhard,"The Applicable Law to Consumer Contracts Made Over the Internet: Consumer Protection Through Private International Law?" Int J L & Info Tech, 1997, vol.5, Issue 2, p.192.

Scott, Hal S, " Corporate Wire Transfers and the Uniform New Payments Code," Nov/1983. Colum. L. Rev. 1664.

Sneddon, Mark, " The Effect of Uniform Commercial Code Article 4A on the Law of International Credit Transfers," 29 Loy. L. A. L. Rev.1107, Apr, 1996.

Sookman, Barry B, Electronic Commerce, Internet and the Law- Survey of the Legal Issues: Part 1," C.T.L.R. 1999, 5 (2), 52.

Spyrelli, C, "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication," (JILT), issue 2, 2002. http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html (obtained on 27/0/2004).

Steennot, Reinhard, "The Single Payment Area," J.I.B.L. 2003, 18(12), 481.

Thevenoz, Luc, "Error and Fraud in Wholesale Funds Transfers: U.C.C. Article 4A and The UNCITRAL Harmonization Process," 42 Ala. L. Rev.881, Winter, 1991.

Thomas, Susan Barkehall, "Electronic Funds Transfer and Fiduciary Fraud," J.B.L. 2005, Jan, 48.

Thunis, Xavier, "Recent Trends Affecting The Banks' Liability During Electronic Funds Transfer," J.I.B.L. 1991,6 (8) 297.

Tufaro, Paul S and Boger, William H, " Electronic Banking in the United States: Evolution not Revolution," 1997, 3(2) CTLR. 70.

Turner, Paul S, "Symposium is the UCC Dead, or Alive and Well? Practitioners' perspectives; the UCC Drafting Process and Six Questions about Article 4A: is there a Need for Revision to the Uniform Funds Transfers Law?" 28 Loy.L.A.L.Rev.351, 1994.

Vroegop, Johanna,"The Time of Payment in Paper-Based and Electronic Funds Transfer Systems," Lloyd's Maritime and Commercial Law Quarterly, 1990, 1(Feb), 64.

Vroegop, Johanna,"The Role of Correspondent Banks in Direct Funds Transfers," Lloyd's Maritime and Commercial Law Quarterly, 1990, 4(Nov), 547.

Walden, Ian,"Data Security and Document Image Processing: Legal Security For Cross-Border Electronic Banking," J.I.B.L.1994, 9 (12), 506.

Walden, Ian, "Regulating Electronic Commerce: European In The Global E-Conomy," E.L.Rev, 2001, 26 (6), 529.

Wo, Lam Wing, " Funds Transfer: A Risk Analysis," J.I.B.L. 1992, 7(1), 16.

Editorial Legislative Comment, " Cross-Border Payments: Amended Directive on EU Credit Transfers," I.B.F.L.1995, 14(2), 11.

## TABLE OF CASES

## UNITED KINGDOM

*Hadley and Another v Baxendale and others*, (1854) 9 Ex.341.

*Hely-Hutchinson* v *Brayhead Ltd* [1968] 1 QB 549.

*Hiron v Pynford South*, [1992] 28 E.G. 112 (QBD (OR)).

*Horne v. Midland Railway*(1872-1873) L.R. 8 C.P. 131.

*Jackson and Another v Royal Banl of Scotland*, [2005] UKHL 3.

*Joachimson* v *Swiss Bank Corporation* (1921) 3 K.B 110.

*Kepitigalla Rubber Estates* v *National Bank of India* [1909] 2K.B1010.

*Libyan Arab Foreign Bank v Banker's Trust Co* [1988] 1 Lloyd's L.R. 259 (Q.B).

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

*Lipkin Gorman* v *Karpnale Ltd* [1991]2 A.C.548.

*London Joint Stock Bank, Limited v Macmillan and Arthur* [1917] 2 K.B.439.

*London Joint Stock Bank, Limited v Macmillan and Arthur* [1918] A.C.777.

*Mardorf Peach & Co Ltd v Attica Sea Carriers Corp of Liberia (The Laconia),* [1977] 2 W.L.R. 286.

*Midland Bank, Ltd.* v *Seymour* [1955] 2 Lloyd's Report.147.

*Minories Finance v Afribank Nigeria Ltd,* [1995] 1 Lloyds's Rep. 134 (QBD (comm)).

*National Bank of Commerce* v *National Westminster Bank* [1990] 2 Lloyd's rep.514.

*National Bank of New Zealand v Walpole and Patterson*, [1975] 2 N.Z.L.R. 7.

*Panatown Ltd v Alfred McAlpine Construction Ltd*, [2000] 4 All ER 97.

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

*R. v Clark (Brian James)*, [2002] 1 Cr. App. R. 14.

*R. v. Preddy* [1996] 2 Cr. App. R. 524 HL.

*Re London & Globe Finance Ltd*, Chancery Division [1903] 1 Ch. 728.

*Robinson v. Harman* (1848) 1 Ex 850

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

*Seven Seas Properties Ltd v. AL-Essa* (No.2) [1993] 1 WLR 1083).

*Simpson v. London and North Western Railway CO* (1876) 1 QBD 274.

*Slingsby and Others* v *District Bank, Ltd* [1931] 41 LI.L. Rep.138.

*Tai Hing Cotten Mill Ltd.* v *Liu Chong Hing Bank Ltd.*and others [1986] A.C.80.

*Tenax Steamship Co Ltd* v *The Brimnes* [1975] 1 Q.B. 929.

*Victoria laundry (Windsor) Ltd v. Newman Industries Ltd* [1949] 2 KB 528.

*Young* v *Grote,* (1827), 4 Bing. 253.

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

**UNITED STATES**

*Banca Commerciale Italiana, New York Branch v. Northern Trust Intern. Banking Corp,* 160 F.3d 90, 36 UCC Rep.Serv.2d 961, 2nd Cir.(N.Y.), Oct 26, 1998 (NO. 97-7633)

*Centre-Point Merchant Bank Ltd* v *American Express Bank Ltd,* 913 F. Supp. 202 ( S.D.N.Y 1996).

*Centre-Point Merchant Bank Ltd* v *American Express Bank Ltd,* WL 1772874 (S.D.N.Y 2000).

*Community Bank, FSB v Stevens Financial Corporation and Creig Stevens* 966 F. Supp. 775 ( N.D. Indiana 1997).

*Evra Corporation v Swiss Bank Corporation* 522 F.Supp.820, District Court N.D. Illinois (1981).

*Evra Corporation v Swiss Bank Corporation,*763 F.2d 951 (7th Cir 1982).

*Grabowski* v *Bank of Boston* 977 F.Supp.111, 119 (D. Massachusetts 1997).

Grain Traders, INC v Citibank, N.A 160 F.3d 97 (2nd Cir 1998).

*Hedged Investment Partners, L.P., et a.l* v *Norwest Bank Minnesota, N.A.* 578 N.W.2d 756(Minn. App 1998).

*Piedmont Resolution, L.L.C v Johnston, Rivlin & Foley,et al.* 999 F. Supp.34 (D. Columbia 1998).

*Sheerbonnet, ltd. v American Express Bank, Ltd* 951 F.Supp.403, ( S.D.N.Y. 1995).

*Re Spectrum Plus Ltd; National Westminster Bank plc v Spectrum Plus Ltd and others,* House of Lords, [2005] UKHL 41.

*Tomaz Mendes Regatos* v *North Fork Bank and New Commercial Bank of New York,* 257 F. Supp.2d 632 (S.D. New York 2003).

*Tomaz Mendes Regatos* v *North Fork Bank and New Commercial Bank of New York* 396 F. 3d 493 ( Court of Appeals 2nd Cir January 2005).

*Tomaz Mendes Regatos* v *North Fork Bank and New Commercial Bank of New York,* 5 N.Y.3d 395, 838 N.E.2d 629, 804 N.Y.S.2d 713, N.Y 2005 (Court of Appeals of New York, October 2005).

## TABLE OF STATUTES

## UNITED KINDOM

## ACTS OF PARLIAMENT

Bill of Exchange Act 1882.

Consumer Credit Act 1974.

Electronic Communications Act 2000.

Fraud Act 2006, Chapter 35.

Interpretation Act 1987.

Law of Property Act 1925.

Theft Act 1968.

## UK REGULATIONS

Cross-Border Credit Transfer Regulations 1999, 1999 No 1876.

Electronic Signature Regulations 2002.

Unfair Terms in Consumer Contracts Regulations 1999.

**UNTED STATES**

Article 4A of the Uniform Commercial Law 1989.
http://www.law.cornell.edu/ucc/4A/ (obtained on 03/02/2004).
http://www.ali.org/

Electronic Funds Transfer Act of 1978.
http://www.fdic.gov/regulations/laws/rules/6500-1350.html
.

**EUROPEAN UNION**

Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, OJ L 043, 14/02/1997 P. 0025 – 0030.

Electronic Signatures Directive 1999/93/EC on a Community Framework for Electronic Signatures, OJ L13 p. 12, 19 January 2000.

**UNCITRAL**

UNCITRAL Model Law in International Credit Transfer 1992.
http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf(obtained on 3/2/2004).

**WEB SITES**

APACS the UK Payments Association, Press Releases, "Latest Figures Show UK Card Fraud Losses Continue to Decline in First Six Months if 2006," 07/11/2006.
http://www.apacs.org.uk/media_centre/press/06_07_11.html (obtained on 09/02/2007).

APACS the UK Payment s Association, "Annual Summary of Clearing Statistics 2006," Facts and Figures, Annual Clearing Statistics.
http://www.apacs.org.uk/resources_publications/documents/annsumm06.pdf (obtained on 08/02/2007)

APACS the UK Payment s Association, "Annual Summary of Clearing Statistics 2004," Facts and Figures, Annual Clearing Statistics.
http://www.apacs.org.uk/ (obtained on 16/10/05).

APACS the UK Payment Association, " Payment Options, Automated Payments 2004"
http://www.apacs.org.uk/payment_options/automated_payments.html# (obtained on 28/11/06)

Bank for International Settlement, "Current Topics in Payment and Settlement Systems," Committee on Payment and Settlement System (BIS), Dec,1999.
http://www.bis.org/publ/cpss35.pdf
http://www.bis.org/index.htm (obtained on 3/2/2004).

Bank for International Settlement, "Payment Systems in United States," CPSS-Red-Book, 2003.
http://www.bis.org/cpss/paysys/UnitedStatesComp.pdf
http://www.bis.org/index.htm (obtained on 3/2/2004).

Bank for International Settlement, "Payment Systems in Euro Area," CPSS-Red-Book,2003.
http://www.bis.org/cpss/paysys/ECBComp.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp-o=2,100000,0
http://www.bis.org/index.htm (obtained on 3/2/2004).

Bank for International Settlement, "Payment Systems in United Kingdom," CPSS-Red-Book,2003.
http://www.bis.org/publ/cpss53p14uk.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp-o=2,100000,0
http://www.bis.org/index.htm (obtained on 3/2/2004).

Bank for International Settlements, "Statistics on Payment and Settlement Systems in Selected Countries," figure for 2002, Prepared by the Committee on Payment and Settlement Systems of the Group of Ten Countries, March 2004.
http://www.bis.org/publ/cpss60.pdf
http://www.bis.org/index.htm (obtained on 3/2/2004).

Claessens Joris, Dem, valentin, De Dock, Danny, Preneel, Bart and Vandewalle, Joos, "On the Security of Today's On-line Electronic Banking Systems," 2002.
http://joris.claessens.ws/pub/stoebs.pdf (obtained on 5/6/2004).

Clearing House Interbank Payments System (CHIPS), "CHIPS Rules and Administrative Procedures," November 2003.
http://www.chips.org/infofiles/CHIPS_rules.pdf

http://www.chips.org (obtained on 3/2/2004).

Clearing House Interbank Payments System (CHIPS), CHIPS Annual Statistics from1970 to 2007.
http://www.chips.org/about/pages/000652.php
http://www.chips.org/(obtained on 08/02/07).

Comptroller of the Currency Administrator of National Banks, "Internet Banking:" Comptroller's Handbook, October 1999.
http://www.occ.treas.gov/handbook/intbank.pdf
http://www.occ.treas.gov (obtained on 25/4/2004).

European Parliament, the Legislative Observatory, Cross-Border Credit Transfers, Procedure Ended and published in the official Journal.
http://www.europarl.europa.eu/oeil/file.jsp?id=87492
http://www.europarl.europa.eu/ (obtained on 24/12/2006)

Federal Deposit Insurance Corporation, Federal Financial Institutions Examination Council, "Authentication in an Electronic Banking Environment," August 8, 2001.
http://www.fdic.gov/news/news/financial/2001/fil0169a.html
http://www.fdic.gov (obtained on 22/6/2004).

Federal Financial Examination Council, "Authentication in an Electronic Banking Environment," August 8, 2001.
http://www.ffiec.gov/pdf/pr080801.pdf
http://www.ffiec.gov (obtained on 24/04/2004).

HSBC, Business Internet Banking (BIB) Terms and Conditions.
http://www.hsbc.co.uk/1/2/business/online-services/terms-conditions (Obtain on 15/05/06).

IT-Analysis, "Fraud Cases up, Financial Losses Down," 29th July 2003.
http://www.it-analysis.com/article.php?articleid=11091
http://www.it-analysis.com (obtained on 4/10/2004).

Law Commission, "The Law Commission and the Scottish Law Commission Report on Unfair Terms in Contracts," 31 December 2004.
http://www.lawcom.gov.uk/docs/lc292.pdf
http://www.lawcom.gov.uk/ (obtained on 16/02/2007)

Organisation for Economic Co-operation and Development, Andreas, Linder, Bill, Cave, Lydia, Deloumax and Oscelyn, Magdeleine, "Trade in Goods and Services: Statistical Trends and Measurement Challenges," OECD Statistics, October 2001, No.1, p.1.
http://www.oecd.org/dataoecd/55/11/2539563.pdf.
http://www.oecd.org/home/ (obtained on 21/01/2004).

Out-Law, "Payment Fraud: Commission sets out Battle Plans," Out-Law. Com/ News, 28/10/2004.
http://www.out-law.com/page-5017
http://www.out-law.com (obtained on 13/10/2005).

Out-Law, "Banks Need Two-Factor Authentication Urgently, Says Forrester," Out-Law. Com, News, 30/03/3005.
http://www.out-law.com/page-5467
http://www.out-law.com (obtained on12/12/2005).

Out-Law, "Lloyds TSB tests Passwords-Generators," Out-Law. Com, News, 17/10/2005.
http://www.out-law.com/page-6234
http://www.out-law.com (obtained on12/12/2005).

Out-Law, "Chip and PIN Sends Card Fraud Online in the UK," Out-Law.Com News, 08/11/2005.
http://www.out-law.com/page-6315
http://www.out-law.com (obtained on12/12/2005).

UNCITRAL, "Electronic Funds Transfer:" Report of the Secretary-General: Electronic Funds
Transfer, UNCITRAL Yearbook Volume XIII: 1982 (A/CN.9/SER.A/1982) p.272.
http://www.uncitral.org/pdf/english/yearbooks/yb-1982-e/vol13-p272-285-e.pdf
http://www.uncitral.org (obtained on 22/6/2004).

UNCITRAL, Electronic Funds Transfer: Report of the Secretary-General: Electronic Fund Transfer, UNCITRAL Yearbook Volume XIII: 1982 (A/CN.9/SER.A/1982) p.272 at p. 275.
http://www.uncitral.org/pdf/english/yearbooks/yb-1982-e/yb_1982_e.pdf
http://www.uncitral.org (obtained on 22/06/2004).

UNCITRAL, "Electronic Funds Transfers, Report of the Secretary- General" (A/CN.9/278), Yearbook of the UNCITRAL, 1986, Vol. XVII, at p.81.
http://www.uncitral.org/pdf/english/yearbooks/yb-1986-e/yb_1986_e.pdf
http://www.uncitral.org (obtained on 12/12/2005).

UNCITRAL, Model Law on International Credit Transfers: compilation of comments by Governments and international organizations (A/CN.9/347 and Add.1) [page 102]. http://www.uncitral.org/english/yearbooks/yb-1991-e/vol22-p102-144-e.pdfindex.htm http://www.uncitral.org (obtained on 22/6/2004).

UNCITRAL, "Report of The UNCITRAL Commission on the Work of its Twenty-Fourth Session, Draft Model Law on International Credit Transfers," Yearbook Vol. XXII 1991, p.5-38. http://www.uncitral.org/pdf/english/yearbooks/yb-1991-e/yb_1991_e.pdf http://www.uncitral.org (obtained on12/12/2005).

UNCITRAL, "International Credit Transfer: Comments on the Draft Model Law on International Credit Transfer: Reports of the Secretary-General" (A/CN.9/346), UNCITRAL yearbook, vol. XXII, 1991, p.52-102. http://www.uncitral.org/pdf/english/yearbooks/yb-1991-e/yb_1991_e.pdf http://www.uncitral.org (obtained on 12/12/2005).

UNCITRAL, "Report of The UNCITRAL Commission on the Work of its Twenty-Fifth Session, Draft Model Law on International Credit Transfers," Yearbook Vol. XXIII 1992, p. 5-14. http://www.uncitral.org/pdf/english/yearbooks/yb-1992-e/yb_1992_e.pdf http://www.uncitral.org (obtained on 12/12/2005).

UNCITRAL, "Possible future work relating to commercial fraud," Note by the Secretariat United Nation Commission on International Trade Law, Thirty- sixth session, Vienna, 30 June-11 July 2003. http://www.uncitral.org/english/sessions/unc/unc-36/acn9-540-e.pdf http://www.uncitral.org (obtained on 8/3/2004).

World Bank, Heinrich, Gregor, "International Initiatives Towards Harmonisation In The Field Of Funds Transfer, payments, payment systems, and Securities Settlements," Basel, 2001, February. http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/InternationalInitiativestowardsharmonisation/$FILE/InternationalInitiativestowardsharmonisation.pdf http://wbln0018.worldbank.org/html (obtained on 28/01/2004).

ZDNet, "Two-Factor Authentication 'not the Solution' to Online Fraud," ZDNet UK, News, 16/03/2005. http://news.zdnet.co.uk/internet/security/0,39020375,39191511,00.htm http://news.zdnet.co.uk (obtained on 06/03/2006).

ZDNet, "Online Banking Security Standard 'by the end of 2005,'" ZDNet UK, News, 17/10/2005.
http://news.zdnet.co.uk/internet/security/0,39020375,39231006,00.htm
http://news.zdnet.co.uk (obtained on 06/02/2006).

ZdNet, "Two-Factor Authentication imminent from Alliance &Leicester," ZDNet UK, News, 28/02/2006.
http://news.zdnet.co.uk/internet/0,39020369,39254930,00.htm
http://news.zdnet.co.uk (obtained on 06/03/2006).

## OFFICAIL REPORTS

### UNITED KINGDOM

Association for Payment Clearing Services, "Yearbook of UK Payment Statistics," 2006.

Association for Payment Clearing Services, "Yearbook of UK Payment Statistics," May, 2004.

HM Treasury, Implementation of the Cross Border Credit Transfer Directive; A Consultation Document, Great Britain, December 1997.

House of Lords, Session 1994-1995 12t Report, "Select Committee on the European Communities, Cross-Border Credit Transfers, with Evidence," 13 June 1995.

"Review Committee on Banking Services: law and practice," report by the Review Committee/ Chairman: R.B. Jack, Vol. XLIX 622-630, 1989.

### EUROPEAN UNOIN

Report from the Commission to the European Parliament and to the Council: On the Application of Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on Cross-Border Credit Transfers, Brussels, 29.11.2002, COM (2002) 663 final.

### UNITED STATES

The official Comment on Article 4A issued by The American Law Institute (ALI) and The National Conference of Commissioners on Uniform State Law (NCCUSL), 1989.

**UNCITRAL**

Report of the Working Group on International Payments on the work of its twenty-first session, UNCITRAL yearbook, vol. XXII, 1991, A/CN.9/341), New York,9-20, July 1990.

UNCITRAL Model Law on International Credit Transfers and explanatory note by the UNCITRAL Secretariat. United Nations, Vienna, 1994, c1999.

**UNCTAD**

UNCTAD, "E-Commerce and Development Report 2001: Trends and Executive Summery," United Nations, New York, 2001.

UNCTAD,"E-Commerce and Development Report 2002," United Nations, New York, 2002.

UNCTAD,"E-Commerce and Development Report 2002," United Nations, New York, 2004.