2016

Electronic Verification of Wire Payment Orders

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

OSGOODE HALL LAW SCHOOL

LEGAL STUDIES RESEARCH PAPER SERIES

Research Paper No. 39 *Volume 12, Issue 8, 2016*

Electronic Verification of Wire Payment Orders

LexisNexis, 2014.

Benjamin Geva

Osgoode Legal Studies Research Paper No. 39
Vol. 12/ Issue. 8/ (2016)

Electronic Verification of Wire Payment Orders

LexisNexis, 2014.

Author(s):
Benjamin Geva
Osgoode Hall Law School
E: BGeva@osgoode.yorku.ca

ESSAYS IN HONOUR OF FRANS MALAN

Former Judge of the Supreme Court of Appeal

Edited by

Coenraad Visser
Professor of Intellectual Property Law in the Department of Mercantile Law, University of South Africa

and

JT Pretorius
Professor of Law in the Department of Mercantile Law, University of South Africa

Assistant editor

MM Koekemoer
Senior Lecturer in the Department of Mercantile Law, University of South Africa

LexisNexis®

Electronic verification of wire payment orders

BENJAMIN GEVA*
York University

INTRODUCTION

At common law, it is well established that on a bank deposit the bank[1] is obligated to the customer as a debtor on a loan[2] and under an 'added . . . obligation . . . to honour the customer's [orders][3] to any amount not exceeding the credit balance'.[4] As for the scope of that 'added . . . obligation', the starting point has been that as 'custodians of the customer's money' providing for 'a safe place of deposit',[5] '[b]ankers can only charge their customers with sums of money paid pursuant to order' as given by the customer.[6] In relation to written payment orders, bankers 'are bound to know the hand-writing of their customers',[7] and certainly their signatures.[8] Hence, banks bear losses caused by payment of forged payment instructions even in the case of a skilful forgery which is unobservable 'in the ordinary course of business'.[9] In sum, being 'the depositary of the customer's money', a banker 'is bound to pay from time to time such sums as the latter may order'; where 'unfortunately [the banker] pays money belonging to the customer upon an order which is not genuine, he must suffer, and to justify

---

* LLB (Jerusalem) LLM SJD (Harvard). Professor of Law at the Osgoode Hall Law School, York University, and Counsel at Torys LLP, Toronto, Canada. This essay draws on, and puts in a broader perspective, B Geva *Law of Electronic Funds Transfers* (loose-leaf) § 2.05[4]. See also B Geva 'Unauthorized electronic funds transfers – comparative aspects', paper presented at the Eighth Biennial Conference of the International Academy of Commercial and Consumer Law, Bar Ilan University, August 1996, published in JS Ziegel (ed) New *Developments in International Commercial and Consumer Law* (1998) 107–133 and B Geva *Bank Collections and Payment Transactions* (2001) 392–421. Research assistance funding was provided in part by the Foundation of the Legal Research of the Canadian Bar Association. For research assistance, I am grateful to Yiyu T Zheng of the Osgoode 2014 graduating class.

1 'Bank' as well as 'banker' are loosely used in this essay interchangeably to connote a person taking deposits from the public and complying with transfer orders of depositors as to the credit available in their respective accounts. Money deposited with banks is typically lent by them in their own name. This feature is not relevant for the present discussion. Historically, the banking business was run by an individual (or individual partners) and hence the person is referred to as 'banker'. At present, it is universal for such business to be incorporated so as to be a 'bank'. Both terms are used here also to cover those who comply with their customers' transfer orders out of a line of credit and not only funds deposited in an account.

2 *Foley v Hill* (1848) 2 HLC 28; 9 ER 1002 (HL).

3 This essay uses 'orders', payment orders', and 'transfer orders' interchangeably. Note that earlier cases dealt with orders embodied in paper instruments, such as cheques and other bills of exchange or drafts, and not in wire payment orders. There is, however, nothing in these cases to limit them to negotiable instruments or any other category of orders. The difference between a manual signature and an electronic authorization is another matter, addressed further below.

4 *Joachimson v Swiss Bank* [1921] 3 KB 110 (CA) at 127 (per Atkin J).

5 *National Bank of Virginia v Nolting* 1897 26 SE 826 (Va SC) at 828 (per Harrison J).

6 *Hall v Fuller* (1825) 5 BC 750 at 757; 108 ER 279 at 282 (per Abbot CJ). The case involved a customer's order subsequently altered without customer's authority.

7 *Smith v Mercer* (1815) 6 Taunt 76 at 86; 128 ER 961 at 965 (per Heath J).

8 James Barr Ames 'The doctrine of *Price* v. *Neal*', in *Lectures on Legal History and Miscellaneous Legal Essays* (1913) 270–271.

9 *Hall v Fuller* supra note 6 at 756 (BC); 282 (ER).

the payment he must show that the order is genuine, not in signature only, but in every respect . . .'[10]

Over the years, albeit less so in connection with consumer accounts,[11] the bank's absolute liability became subject to exceptions. Particularly, bypassing a classical text explicitly to the contrary,[12] it had been recognized that a customer's fault can lead to the forgery of the customer's own signature and hence to forgery losses. The door was thus opened for a bank which paid over an unauthorized payment order to avoid liability not only where the customer had been aware of the unauthorized order[13] but also by invoking the customer's negligence in facilitating the issue of the unauthorized payment instructions. In the United States of America,[14] and subsequently in South Africa,[15] the bank's right is codified. In England[16] and Canada,[17] such a right must be provided by contract.[18] Accordingly, the rule was modified to make the bank's liability less absolute so as to be avoided where fault lay with the customer. It was thus said that '[i]f the bank pays money on a forged check, no matter under what circumstances of caution, or however honest the belief in its genuineness, if the depositor himself be free of blame, and has done nothing to mislead the bank, all the loss must be borne by the bank, for it acts at its peril, and pays out its own funds, and not those of the depositor'.[19]

Nonetheless, there are circumstances in which a bank may seek to be released from liability for payment of unauthorized orders even where neither knowledge nor negligence can be attributed to the customer. Thus, in practice, a customer's payment order is transmitted to its[20] bank either by the delivery of a piece of paper or electronically.[21] Sender's authority is thus verified by the receiving bank[22] with the view of authenticating the communication either by

---

[10] At 757 (BC); 282 (ER) (per Bayley J).

[11] See, for example, the Electronic Fund Transfer Act (EFTA) 15 USC §§ 1693 et seq in the United States of America, where a consumer's exposure is limited regardless of negligence facilitating an unauthorized funds transfer.

[12] RJ Pothier *Traité du contract du change* (new ed by JB Hutteau (ed)) (1809) 55–68. His overall position is explored in Benjamin Geva *Bank Collections and Payment Transactions* (2001) 349–351. He analysed the point as an issue under mandate law which is the general framework governing the execution and collection of payment orders in South Africa. See FR Malan and JT Pretorius 'Bills of Exchange, Cheques and Promissory Notes' § 7, around note 55 in ABLU'96 (*Annual Banking Law Update* 1996). On the particular point in the accompanying text his view is certainly anachronistic.

[13] See, for example, *Greenwood v Martins Bank Ltd* [1933] AC 5 (HL); *Ewing v Dominion Bank* (1905) 35 SCR 133 (Canada).

[14] See UCC s 3-406.

[15] Section 72B of the Bills of Exchange Act 34 of 1964 (among other provisions), inserted by the Bills of Exchange Amendment Act 56 of 2000.

[16] See, for example, *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1985] 3 WLR 317 (PC).

[17] See, for example, *Canadian Pacific Hotels Ltd v Bank of Montreal* (1987) 40 DLR (4th) 385 (SCC).

[18] Much of the discussion and even a resulting statutory provision (such as UCC 4-406 in the United States of America) on the customer's negligence addresses the specific obligation of examining and verifying banks' periodic statements and advising the bank of any discrepancy (including an unauthorized payment). The breach of such a duty may reduce the bank's chances of identifying and recovering from the wrongdoer and allow a repeating wrongdoer to issue future unauthorized orders.

[19] *Hardy v Chesapeake Bank* (1879) 51 Md 562 *11 (per Alvey J).

[20] Most business customers are incorporated.

[21] In principle, communication may be oral, except that typically an oral communication is followed by either a signed written confirmation or a verification according to an agreed-upon 'security procedure' of the type discussed further below.

[22] In the footsteps of UCC s 4A-103, throughout this essay, the terms 'sender' and 'receiving bank' are the parties to a 'payment order' issued in the course of a wire transfer. On UCC article 4A in the United States of America, see, generally, note 26 below.

the examination of the signature or according to a security procedure. A signature is individual to each person so that its verification confirms the identity of the signer. This is, of course, correct also in relation to a corporate customer which obligates itself by the signature of designated signatories whose signatures are on file with the bank. At the same time, the verification according to a security procedure serves as a legitimization of the communication without the identification of the individual sender who actually issued it.

In the absence of a manual signature, banks are unable to link a payment order with an individual who issued it. True, banks remain perceived as 'custodians of the customer's money' providing for 'a safe place of deposit'.[23] At the same time, where the identification of the issuer cannot be ascertained by the bank, the rationale for the bank's absolute liability for an unauthorized payment order, as stated above, becomes significantly weaker. Unsurprisingly then, American authorities dealing with negotiable instruments have given full effect to corporate resolutions authorizing the use of facsimile signatures to bind corporate entities.[24] This must be correct in England as well.[25]

Acting on a contractually agreed electronic authorization is in principle not different from acting on a facsimile signature affixed to a payment instrument on which the bank is authorized to act according to the customer agreement. In either case the bank is unable to associate the authorization with a particular person. Hence, the bank may similarly be justified in including in the customer agreement a term authorizing the bank to act on a payment order that was issued according to the agreed-upon security procedures. Effectively, such a term is designed to estop the corporate customer from pleading that the person who affixed the facsimile signature or inserted the card and used the right code was not authorized to do so.

For its part, however, a customer who followed the security procedure in issuing a payment order expects the procedure to be reliable and that the bank will properly verify as to whether it has been followed. In a sense, this lowers the bank's verification duty from being absolute to that of due care. Indeed, in the United States of America, prior to the adoption of article 4A of the Uniform Commercial Code (UCC),[26] *Walker v Texas Commerce Bank*[27] stated that in acting on a payment order the receiving bank is under a duty to 'implement commercially reasonable internal procedures designed to process [a payment order] in accordance with [the sender's] instructions, to verify the accuracy of, and compliance with, instructions, to detect and minimize inaccuracy, and act diligently to remedy errors'.[28] This is in line with the receiving bank's 'duty to use reasonable care and skill' in carrying out instructions contained in a payment order, set out in England in *Royal Products Ltd v Midland Bank Ltd.*[29] Both such statements reflect a principle broad enough to cover the receiving bank's duties in carrying out the verification of the authenticity of the payment instructions.

---

[23] *National Bank of Virginia v Nolting* supra note 5.

[24] See, for example, *Perini Corp v First National Bank of Habersham City* 553 F 2d 398 (5th Cir Ga 1977).

[25] This is so, as under s 91(2) of the Bills of Exchange Act 1882, the seal of a corporation may be an equivalent to a signature. True, *Chalmers and Guest on Bills of Exchange and Promissory Notes* 16 ed by AG Guest (2005) questions (at 154 ¶ 3-023) the adequacy of 'a lithograph or a stamped facsimile of a signature' and yet arguably this is not in a context of an authorizing resolution.

[26] Article 4A of the Uniform Commercial Code was approved in 1989 by the American Law Institute (ALI) and the National Conference of Commissioners on Uniform State Law (NCCUSL) for adoption by the various states. By March 1996 it had been adopted throughout the United States of America.

[27] 635 F Supp 678 (SD Tex 1986).

[28] At 682.

[29] [1981] 2 Lloyd's LR 194 198 (QB).

In endeavouring to meet negligent customers' pleas designed to reallocate unauthorized order losses, non-negligent banks may successfully rely on their own lack on negligence.[30] In some cases, non-negligent banks may, however, wish to escape liability even where customers were not negligent. Such is the case, for example, where banks provided a reliable security procedure which they diligently followed. In turn, customers wish to remind banks that they are 'custodians of the customer's money' providing for 'a safe place of deposit',[31] so as to leave banks liable, at least as long as no fault (or even no gross negligence) has been attributed to the customer.

Against the background of very little case law, it cannot be anticipated that under the common law a proper balance between the legitimate expectations of the bank and the customer will be established soon enough to satisfy certainty. Left to their own mischief, and without violating rules that preclude them from disclaiming their own due care obligations,[32] banks successfully managed to invoke contractual terms that allowed them to escape liability not only when the customer was negligent. Rather, such terms released banks also when they acted on a counterfeit facsimile signature placed on a cheque[33] or counterfeit wire instructions[34] as long as they were effectively acting without knowledge of the ingenuity, or at least without gross negligence. This was so even if the fraudster was a complete outsider to the customer's organization who accessed relevant information without any fault of the customer or someone in its organization. This, however, appears to go too far in overlooking banks' traditional role according to which they are perceived to be 'custodians of the customer's money' providing for 'a safe place of deposit'.[35]

Article 4A of the UCC contains an elaborate scheme of loss allocation for unauthorized wire transfers[36] which purports to achieve the right balance.[37] Briefly stated, under that scheme, the customer is liable to the receiving bank for the amount of any authorized payment order for which the customer is bound under the law of agency. The customer is also liable for the amount of any payment order, including an unauthorized one, whose authenticity was properly verified pursuant to a commercially reasonable security procedure agreed upon between the customer and the bank. However, such an unauthorized order does not bind the customer where it is otherwise agreed, or where the customer proves that the order was not caused by a person other than an interloper. Accordingly, the risk of an unauthorized payment order falls initially on the bank. Such risk shifts to the customer if the bank proves its good-faith compliance with an agreed-upon commercially reasonable security procedure. The risk shifts back to the bank when the loss is proved by the customer to have been caused by an interloper or is allocated to the bank by agreement.

This essay assesses the success of the UCC article 4A scheme in implementing a correct balance between the expectations of the bank and customers. It discusses the statutory provisions and their interpretation by case law. It concludes that, in the final analysis, the scheme under UCC article 4A is a great leap forward. At the same time, the essay calls for an

[30] A bank's negligence allows a negligent customer to shift at least part of the loss back to the bank: see, for example, UCC ss 3-406 and 4-406 in the United States of America.

[31] *National Bank of Virginia v Nolting* supra note 5.

[32] As, for example, under UCC s 4-103(*a*) in the United States of America.

[33] *Jefferson Parish School Board v First Commerce Corp* 669 So 2d 1298 (La Ct App), effectively criticized by James Steven Rogers *The End of Negotiable Instruments* (2012) 135–137.

[34] *Stan-Ka Auto Corp Ltd v Blinkova* [1998] OJ No 1047 (Ont CJ Gen Div) (QL(OJ) Spence J).

[35] *National Bank of Virginia v Nolting* supra note 5.

[36] UCC art 4A, wire and automated clearing house (ACH) credit transfers (see Prefatory Note to UCC art 4A). This essay focuses on wire transfers typically processed over large-value payment systems.

[37] UCC ss 4A-201–204.

improvement in statutory language, as well as for an increase in courts' awareness of pertinent policy considerations.

IS VERIFIED PAYMENT ORDER 'AUTHORIZED'?

Under section 4A-202(*a*), '[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 the laws of agency'.[38] Authority can be given to the bank according to the terms of an agreement previously entered into between the bank and customer.[39] This will typically be a framework agreement to govern future payment orders. Authority could, however, also be given to the bank by the customer on an ad hoc basis, in the absence of a pre-existing agreement, and even contrary to the terms of such an agreement.[40]

It is, however, recognized that where transmission of the payment order is made electronically, which is the common case in the wire-transfer business, agency concepts are not sufficiently helpful to ascertain the sender's authority. The receiving bank which 'may be required to act on the basis of a message that appears on a computer screen' is relying on verification pursuant to a security procedure, and not on the authority of any particular person.[41] Indeed, a security procedure is not necessarily limited to a computerized environment and might apply to a communication that is transmitted by telephone or in writing.[42] However, in connection with an electronic communication, it is not only that '[p]rudent banking practice may require that security procedures be utilized'.[43] Rather, effectively, a security procedure in such a case is indispensable. In fact, to bypass security procedures in an electronic environment, a receiving bank should have agreed with the customer as to what facts constitute authorization to the bank to act on payment orders purporting to be sent on the customer's behalf. Hence, a security procedure is predominantly used for the verification of an electronic communication. It is in this context that security procedures are discussed in this essay.

Verification is designed to link the payment order to its source so as to 'authenticate' it. Effectively, proof of verification pursuant to a security procedure is a step towards proving authority.[44] In fact, and without using any language to that effect, article 4A creates a rebuttable presumption that a properly verified payment order has been authorized. Presumption

---

[38] It goes without saying that a genuine payment order issued by a natural person in his or her own name is binding on that person, and as between himself or herself and the receiving bank is authorized in the sense of s 4A-202(*a*).

[39] The construction of such terms was addressed in, for example, *Dark Hall Productions LLC v Bank of America NA* 2012 WL 6202186 (Cal App 2 Dist).

[40] As was alleged (albeit disproved) in *Frungillo v Imperia Entm't Inc* 2009 US Dist LEXIS 89863 (DNJ 2009), where anyway the payment discharged the originator's obligation.

[41] Official Comment 1 to s 4A-203.

[42] See Official Comment to s 4A-201, and, for example, *Chavez v Mercantil Commercial Bank* 701 F 3d 896 (CA 11 (Fla) 2012), *rvs'g* 2011 US Dist LEXIS 126309 (SD Fla 1 Nov 2011); *Braga Filho v Interaudi Bank* 2008 US Dist LEXIS 31443 (SDNY 2008); *Regatos v North Fork Bank* 396 F 3d 493 (2d Cir 2005) (for earlier proceedings in the same case, see 257 F Supp 2d 632 (SDNY 2003) and 838 NE 2d 629 (NY 2005)).

[43] Official Comment 3 to s 4A-203. For the distinction between authorized and verified payment orders, and for the fact that security procedures determine verification but not authorization, see *Hedged Investment Partners v Norwest Bank* 578 NW 2d 765 (Minn Ct App 1998).

[44] Possibly, this is the role of verification for consumer payment orders under the EFTA, 15 USC §§ 1693 et seq (ss 903(11) and 909) and Regulation E, 12 CFR § 205 (s 205.2(*m*) and 205.6) under which an unauthorized fund transfer is to be distinguished from an authorized one; no 'intermediate' category of 'verified' fund transfer is said to exist. Hence, proof of verification is one step towards proving authority.

may, however, be rebutted only by the customer's proving a specified set of facts; customer's proof for mere lack of authority will not suffice. To that end, section 4A-202 can be seen as providing in subsections (*b*) and (*c*) for the elements to be proven by a bank wishing to benefit from the presumption, either where no authorization was given, or where there is a genuine factual issue as to its existence.[45] At the same time, from the same perspective, section 4A-203 can be seen as dealing with what is to be proved by a customer wishing to rebut the presumption.

Instead of referring to a presumption of authority, article 4A speaks, however, of the binding effect of a payment order that was proved to be verified pursuant to a security procedure, and, conversely, of its unenforceability, if certain facts are nonetheless proved by the customer. Accordingly, the risk of an unauthorized payment order falls initially on the bank. Such risk shifts to the customer if the bank proves its good-faith compliance with an agreed-upon commercially reasonable security procedure. The risk shifts back to the bank when the loss is proved by the customer to have been caused by an interloper or is allocated to the bank by agreement.[46]

VERIFICATION ACCORDING TO AGREED SECURITY PROCEDURE

Under section 4A-201, a 'security procedure' must be established by agreement between a customer and a receiving bank. 'The term does not apply to procedures that the receiving bank may follow unilaterally in processing payment orders'.[47] The pertinent agreement ought to be established for the purpose of 'verifying that a payment order or communication amending or cancelling, a payment order is that of the customer.'[48] To the same end, under section 4A-202(*b*), effective verification requires an agreement between the bank and the customer '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'.

The agreement providing for the security procedures need not be express or in writing; it could be oral or even implied from a course of dealing.[49] For evidentiary purposes, however, it may be more efficient for a bank to reduce such an agreement to writing. A written agreement is nevertheless needed where the customer refuses a security procedure offered by the bank and chooses its own, and the bank wishes to benefit from the presumption under section 4A-202(*c*) as to the commercial reasonableness of the security procedure chosen by the customer. Typically, such a written agreement will bind the customer to any payment order whose

---

[45] As in *Insoftvision LLC v MB Financial Bank* 2011 WL 4036134 (ND Ill).

[46] For a 'textbook' exposition, see, for example, *Choice Escrow and Land Title LLC v BancorpSouth Bank* 2013 WL 1121339 (WD Mo).

[47] Official Comment to s 4A-201. This principle was applied in *Skyline Int'l Dev v Citibank* 706 NE 2d 942 (Ill App 1998). See also *Utility Supply Co v AVB Bank* 2010 US Dist LEXIS 126948 (ND Okla 2010). As well, in *Grabowski v Bank of Boston* 997 F Supp 130 (D Mass 1997), the Court drew the obvious conclusion that an agreement between the bank and the person alleging to be the customer's authorized agent is insufficient to establish effective 'security procedures'.

[48] Under s 4A-201, the agreement may be established for the purpose of 'detecting error in the transmission or the content of the payment order or communication'. This, however, is another matter, unrelated to the authenticity of a payment order sent in the customer's name, governed by s 4A-205.

[49] Under s 1-201(*a*)(3). 'Agreement' connotes 'the bargain of the parties in fact, as found in their language or inferred from other circumstances, including course of performance, course of dealing, or usage of trade'. 'Course of dealing' is defined in s 1-205(1) as 'a sequence of previous conduct between the parties to a particular transaction which is fairly to be regarded as establishing a common basis of understanding for interpreting their expressions and other conduct.' Corresponding Revised Section 1-303(*b*) is almost verbatim.

authenticity was verified by the bank in good faith and pursuant to the inferior security procedure chosen by the customer.[50]

From the customer's viewpoint, under section 4A-203(*a*)(1), an express written agreement is required to have the risk of an unauthorized payment order shifted back to the bank, notwithstanding the use of the commercially reasonable security procedure. In addition, a written agreement or instruction of the customer is required to impose restrictions on the use of security procedures with respect to the acceptance of designated payment orders under section 4A-202(*b*).

Where a customer 'expressly agreed to the use of security passcodes . . . and it agreed by course of performance to the use of challenge questions, having cooperated in setting up answers to such question', the court held that 'there [was] no genuine dispute that it agreed to the core security procedures visible to users'.[51] It was also held that a security procedure chosen unilaterally by the bank pursuant to the customer's authorization is established by agreement.[52] As well, 'agreement' may be evidenced by the customer's knowledge that the bank uses the procedure to verify payment orders and is not breached by the bank by merely unilaterally changing the procedure name.[53]

There are precedents allowing the bank to rely on the customer's agreement and acknowledgement of the commercial reasonableness of the 'security procedure'.[54] Arguably, however, such an agreement is, contrary to section 4A-202(*f*), an invalid waiver by the customer of its rights under section 4A-202. Thereunder, liability for unauthorized payment orders is limited only to those properly verified according to what the court views, rather than what the customer concedes to be, a 'commercially reasonable' security procedure.

Where a valid agreement exists, under section 4A-202(*b*), a payment order received by the bank is effective as the order of the customer, whether or not authorized, where it was accepted by the bank in good faith and upon compliance with an agreed-upon commercially reasonable security procedure.[55]

As for its contents, under section 4A-201, '[a] security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices'. At the same time, '[c]omparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a

---

[50] Query if by such agreement the customer does not waive its right (under s 4A-203(*a*)(2)) to avoid liability by proving that the fraud was perpetrated by an interloper (such as an employee of the bank). See Paul S Turner 'The UCC drafting process and six questions about article 4A: is there a need for revisions to the Uniform Funds Transfer Law?' (1994) 28 *Loyola of Los Angeles LR* 351 at 360–363.

[51] *Patco Constr Co v People's United Bank* 2011 US Dist LEXIS 58112 at *104 (D Me 2011), *revs'd on other grounds*, 684 F 3d 197 (1st Cir 2012).

[52] Certainly, as long as it is commercially reasonable, as required from any security procedure (see further below), such a security procedure is valid. See *Braga Filho v Interaudi Bank* supra note 42, which was distinguished in *Chavez v Mercantil Commercial Bank* supra note 42, where the majority did not read the particular agreement as authorizing the bank to choose a 'security procedure'.

[53] *Experi-Metal Inc v Comerica Bank* 2010 US Dist LEXIS 68149 (ED Mich 2010). An 'agreement' was found to exist in that case even where knowledge of the procedure by the customer was in relation to payments *received* and not *sent* by it.

[54] For example, *Experi-Metal v Comerica Bank* supra note 53; *Transamerica Logistic Inc v JPMorgan Chase Bank NA* 2008 US Dist LEXIS 112708 (SD Tex 2008).

[55] Compare *All American Siding & Windows v Bank of America* 367 SW 3d 490 (Tex App 2012), where the court determined only the existence of an agreement. However, the chance is that in the facts of the case the security procedure (consisting of logging in using the company ID and a user ID with each user having a specific 'digital certificate') was in any event commercially reasonable.

security procedure'.[56] Mere voice recognition is not, by itself, a security procedure. Nevertheless, requiring confirmation by providing 'user information' of an authorized officer is a valid element of an otherwise computerized effective security procedure.[57]

Under section 4A-202(*c*), commercial reasonableness of a security procedure is a question of law. As explained in Comment 4 to section 4A-203: 'It 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.'

In determining the commercial reasonableness of a security procedure, consideration will be given to '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, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated'.[58]

Taking into account that '[v]erification entails labor and equipment costs that can vary greatly depending upon the degree of security that is sought', Comment 4 to section 4A-203 states:

> 'A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge . . . would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard. On the other hand, a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable.'

While whether a particular security procedure is 'commercially reasonable' is a question of law, compliance by the receiving bank with the procedure is, in each case, a question of fact.[59]

Where the customer rejects a commercially reasonable security procedure offered by the bank in favour of a security procedure of its own choice, the offering bank may benefit from a presumption of commercial reasonableness attributed to the security procedure selected by the customer. Thus, under section 4A-202(*c*):

> '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, a 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 procedure chosen by the customer.'

This recognizes that an informed customer may refuse a commercially reasonable security procedure offered by the bank and insist on using a higher risk and more convenient or cheaper procedure. In such a case, the loss from an unauthorized but properly verified payment order is not shifted to the bank, even if the security procedure chosen by the customer does not meet the commercial reasonableness standard.[60] Nonetheless, to be protected from

---

[56] Section 4A-201. At the same time, a comparison of a test key will constitute a security procedure. *See ReAmerica SA v Wells Fargo Bank Int'l* 2008 US Dist LEXIS 30614 (SDNY 2008), *aff'd ReAmerica SA v Wells Fargo Bank Int'l* 577 F 3d 102 at 106 (2d Cir 2009).

[57] *Experi-Metal v Comerica Bank* supra note 53.

[58] Section 4A-202(*c*). For a detailed analysis, see, for example, *Patco Constr v People's United Bank* supra note 51 (2011) at *108, as well the reversing judgment supra note 51 (2012) at 210–11, reaching the reverse conclusion in the facts of the case.

[59] See *Centre-Point Merchant Bank v American Express Bank* 43 UCC Rep Serv 2d 372 (SDNY 2000).

[60] Official Comment 4 to s 4A-203.

the failure of a security procedure chosen by the customer, the bank must have originally offered the customer a commercially reasonable security procedure.

In *Choice Escrow and Land Title v BankcorpSouth*,[61] 'on two different occasions' the customer 'was offered the opportunity to employ 'Dual Control'[62] in sending payment orders. Such procedure required that each electronic wire transfer be initiated by two individuals acting on behalf of the customer, each having a distinct ID and acting separately. Fearing that reliance on the need to constantly have two authorized employees present in the office would prove costly, the customer declined and selected a system that by itself was commercially reasonable and yet did not prevent a hacker from diverting funds overseas. Recognizing that '[t]he tension in modern society between security and convenience is on full display in this litigation',[63] the court nevertheless found that in any event two authorized employees were in the office at the same time. Thus effectively taking into account 'circumstances of the customer known to the bank' as required under section 4A-202(*b*), the court held that the 'Dual Control' procedure was commercially reasonable.

To benefit from the protection under section 4A-202(*b*) for an unauthorized but verified payment order, the bank must prove[64] that it accepted the payment order in good faith, that it complied with the commercially reasonable security procedure,[65] and that it accepted the payment order 'in compliance with . . . any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer'.[66] However, the bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.[67]

Under section 4A-105(*a*)(6), 'good faith' connotes honesty in fact and the observance of reasonable commercial standards of fair dealing. While the first prong—'honesty in fact'—is subjective, the second prong—'the observance of reasonable commercial standards of fair dealing'—is objective.[68] Particularly as to the latter, it is not all that clear what the bank has to show in order to prove that in accepting a payment order it acted in good faith.[69] It was argued in *Experi-Metal Inc v Comerica Bank*[70] that the acceptance by a receiving bank of instructions to pay to unusual destinations and at an accelerated frequency indicated a breach of this condition. Initially, in finding a genuine issue of material fact with respect to that point, the court did not elaborate on the knowledge requirement for the receiving bank, particularly in the context of a mechanical operation such as the issue of payment orders

---

[61] *Choice Escrow and Land Title v BancorpSouth Bank* supra note 46.

[62] At *6.

[63] At *9.

[64] Under s 4A-105(*a*)(7), 'prove' with respect to a fact connotes assuming the burden of establishing that fact. Under s 1-201(8), 'burden of establishing' a fact connotes the burden of persuading the triers of fact that the existence of that fact is more probable than its non-existence

[65] See, for example, *Utility Supply v AVB Bank* supra note 47, where the court was prepared to treat the customer's negligence claim with respect to the receiving bank's failure to follow its own security procedure as an action for the breach of the agreed-upon commercially reasonable security procedure.

[66] Section 4A-202(*b*)(ii). Compliance with security procedures is an important issue of fact that precludes summary judgment in the bank's favour: see *Schroeder v Capital One Financial Corp* 665 F Supp 2d 219 (EDNY 2009).

[67] Section 4A-202(*b*). See, for example, *Experi-Metal v Comerica Bank* supra note 53.

[68] *Experi-Metal Inc v Comerica Bank* 2011 US Dist LEXIS 62677 (ED Mich 13 June 2011), *aff'ng Experi-Metal v Comerica Bank* supra note 53.

[69] Turner op cit note 51 at 363–364.

[70] *Experi-Metal v Comerica Bank* supra note 53.

verified according to agreed-upon security procedures. Ultimately, however, the trier of fact accepted the argument. He pointed at 'the volume and frequency of the payment orders and the book transfers that enabled the criminal to fund those orders; the $5 million overdraft created by those book transfers in what is regularly a zero balance account; [the originator]'s limited prior wire activity; the destinations and beneficiaries of the funds; and [the receiving bank]'s knowledge of prior and the current phishing attempts'.[71] In the absence of evidence presented by the receiving bank conveying the commercially reasonable standards of fair dealing,[72] he was thus 'inclined to find that a bank dealing fairly with its customer . . . would have detected and/or stopped the fraudulent wire activity earlier'.[73]

LOSS ALLOCATION UNDER THE STATUTE

Under section 4A-202(*b*), 'a payment order . . . is effective as the order of the customer, whether or not authorized', if it is verified pursuant to the agreed-upon security procedure. The effect of this provision is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure.[74]

Section 4A-203 provides for two exceptions. The first reflects the limits to the rationale of section 4A-202(*b*). The second recognizes the parties' power to contract out of some provisions of article 4A. Thus, underlying the customer's responsibility for an unauthorized but verified payment order is the assumption that information on the security procedure facilitating compliance and successful verification is likely to have been made available to the wrongdoer by the customer. To that end, section 4A-203(*a*)(2) effectively places on the customer an obligation to safeguard confidential security information to prevent breaches of the agreed-upon security procedures.[75] Under that provision, the customer may avoid the loss resulting from payment of an unauthorized but verified payment order by proving that neither breach of trust nor a leak occurred at its end. This means that the customer is not responsible for the amount of the payment order if it proves that—

> '. . . the order was not caused, directly or indirectly, by a person (i) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or (ii) who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault. Information includes any access device, computer software, or the like.'

The customer must then prove that the order was not caused by a person other than an interloper.[76] Evidence needed by the customer in order to meet the required burden of proof[77] is likely to be generated by the criminal and internal investigations conducted in the aftermath of the breach of security.[78]

---

[71] At *37–38.

[72] At *38.

[73] Ibid. Conversely, in *Patco Constr v People's United Bank* supra note 51 (2011), *rvrs'd* supra note 51 (2012), a prompt advice to the customer sufficed.

[74] Official Comment 5 to s 4A-203.

[75] *Travelers Cas & Sur Co of America v Bank of America NA* 2010 US Dist LEXIS 30817 (ND Ill).

[76] Or, as in *Transamerica Logistic v JPMorgan Chase Bank* supra note 54, the customer must prove that the disputed transfer orders 'were caused by a person entrusted by [the customer] to order wire transfers or by an unauthorized person who gained access to [the customer's] User ID and password from a source controlled by [the customer].'

[77] See ss 1-201(8) and 4A-105(*a*)(7).

[78] See Official Comment 5 to s 4A-203.

Section 4A-203(*a*)(1) provides for a second exception to the customer's responsibility for an unauthorized but properly verified payment order. The loss resulting from such a payment may be shifted, in whole or in part, to the receiving bank by express written agreement between the bank and the customer.

In attempting to shift to its bank losses caused by unauthorized but properly verified payment orders, a customer may however encounter several difficulties.

In the first instance, banks are unlikely to expressly agree in writing to assume this risk, as mandated by the second exception.

Secondly, a few statutory limitations and ambiguities exist in the quoted language of section 4A-203(*a*)(2), providing for the first exception. *(a)* It is true that, under clause (i), it is not loss caused by any employee of the customer that appears to fasten liability on the customer; rather, it must be loss caused by a 'person . . . entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure'. At the same time, however, under clause (ii), the customer is also bound by loss caused by any 'person . . . who obtained access to transmitting facilities of the customer'. Thus, having 'obtained access to transmitting facilities of the customer', an employee not covered by clause (i) may nevertheless fall under clause (ii). *(b)* Regardless, is the 'obtained access to transmitting facilities' in clause (ii) (which precludes the customer from avoiding liability) limited to physical access, or rather, does it cover also 'virtual' access from a remote terminal or computer? Official Comment 5 to section 4A-203 speaks of 'access to transmitting facilities through an access device or other software', which supports the 'virtual' access interpretation.[79] Whether access must be given by the customer voluntarily, so that at least in the absence of fault by the customer, a hacker will not be a person covered by clause (ii), may be an open question.[80] Even if the customer's responsibility is limited to cases where access is voluntarily given, there may be circumstances under which 'access' is fraudulently induced, negligently given, or inadvertently surrendered for purposes other than the dispatch of a payment order purportedly by the customer. What is required under clause (ii) is causation by either the obtainment of access to the customer's transmitting facilities, or the obtainment from a source controlled by the customer (and without the receiving bank's authority) of information facilitating a breach of the security procedure. Fault of the customer is said not to be a factor only with respect to the second prong, that of the obtainment of information and not the obtainment to access to facilities. However, there is no reason to suppose that the obtainment of access to the customer's facility by fraudulently inducing the customer or taking advantage of the customer's negligence will excuse the customer. *(c)* Clause (ii) allocates responsibility to the customer for a payment order caused by a person 'who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault'. Information is broadly defined to include 'any access device, computer software, or the like'. This seems to fasten responsibility to the customer only where loss caused by information originated in an area under its control. But how far does the customer's control

[79] See, for example, RW Ludwig, S Scanio and S Szary 'Malware and fraudulent electronic funds transfers: who bears the loss?' (2010) 16 *Fidelity LJ* 101.

[80] A negative answer—meaning that access preventing the customer to avoid liability need not necessarily be given voluntarily—was assumed by the court in *Transamerica Logistic v JPMorgan Chase Bank* supra note 54. In that case, the user ID and password had allegedly been saved to a laptop that was confiscated by law enforcement officials. The court assumed that this prevented the customer from avoiding liability for payment orders subsequently issued and properly verified by the receiving bank under an agreed-upon commercially reasonable security procedure.

extend? What about access obtained, or information received, from a third-party communication system for the transmittal of payment orders to the bank? Under section 4A-206, such a system 'is deemed to be an agent of the sender'. As such, does the system become 'a source controlled by the customer', and its transmitting facilities become those 'of the customer', so as to make the customer responsible for losses caused by breach of security in such a system? Such a conclusion is not inevitable and in my view ought to be rejected; agency under section 4A-206 is to be limited to the terms of a payment order actually transmitted by the customer through the system. Nevertheless, this view may not be universally shared and the question remains open.

Thirdly, allocation of losses caused by verified unauthorized orders under article 4A is asymmetric. Under section 4A-202, the bank avoids liability by proving compliance with an agreed-upon commercially reasonable security procedure and other contracts. Conversely, to shift liability back to the bank, and in the absence of (an unlikely) contract to the contrary, the customer is required to prove under section 4A-203, that the payment order was not caused 'directly or indirectly' by a breach of security at its own end. The latter set of facts is much harder to prove than compliance with the security procedure. Certainly, the customer will not avoid liability by merely proving due diligence or compliance with commercially reasonable standards in controlling both access to its transmittal facilities and information held by a source controlled by it. Furthermore, as will be shown below, according to *Patco Constr v People's United Bank*,[81] in principle, even where the bank's security procedure is not found to be commercially reasonable, a customer may be found to be in breach of a duty to the bank and thus bear the loss. It was even argued in the court below in that case that a commercially reasonable agreed-upon security procedure unintentionally weakened by the addition to it by the bank of new elements (that effectively compromised the elements agreed upon) remains commercially reasonable. Unless such practice undermines the good-faith compliance with the agreed security procedure, there may not be a way for the customer to introduce this aspect into the 'equation'.[82] However, as discussed below, the Court of Appeal ultimately declined to find the security procedure, together with the additional elements, to be commercially reasonable.

In *Elite Investigations v Bank of New York*,[83] Elite's payment orders were to be issued by inputting, through a third-party communication system,[84] the security code that appeared on a credit card of the company president, together with the president's social security number and date of birth. This must be taken to form a 'security procedure' the commercial reasonableness of which was not questioned by the court. A fraudulent Elite employee, who had been removed from the signature card of the company as a result of an earlier fraud, but who nevertheless remained authorized to review its bank and charge-card statements, and who was entrusted with a corporate charge card, initiated electronic funds transfers under the president's name and misappropriated the funds for his own personal use.[85] Elite sought to challenge the debits to its bank account on the basis of alleged bank's duties to ensure that the

[81] Supra note 51 (2012) at 214–215.

[82] *Patco Constr v People's United Bank* supra note 51 (2011).

[83] *Elite Investigations v Bank of NY* 13 Misc 3d 1233A (NY Sup Ct 2006).

[84] In the facts of the case, the third-party communication system consisted of American Express and the bank it used. For a communication system as an agent of the sender, see s 4A-206. In the facts of the case, each payment order initiated an ACH payment that the Court assumed to be governed by art 4A.

[85] The consequences of the corporate customer's failure to give a timely notice of the contested debits, caused in the facts of the case by the involvement of the fraud instigator in the review of the bank statement, would have been a matter governed by s 4A-204. The provision is, however, limited to unauthorized or unverified payment orders in respect of which the bank is liable in the first place.

fraudulent employee had no access to its account as he had been removed from the signatory card. Concluding that the bank had no practical way of determining who initiated the funds transfers and whether the payment orders were authorized, the court summarily dismissed the action.

In fact, the relevant issue was not whether the payment orders were authorized, but rather whether the corporate customer could overcome the bank's reliance on verification pursuant to a commercially reasonable security procedure. In the facts of the case, it is unlikely that the corporate customer could have proven that the payment orders were not caused other than by an interloper in the sense of section 4A-203(*a*)(2). Thus, the action may have correctly been summarily dismissed, though for the wrong reasons.

PATCO CONSTRUCTION V PEOPLE'S UNITED BANK EXAMINED

Patco Construction v People's United Bank[86] explored major issues in the interpretation of section 4A-202(*b*) and the resulting loss allocation under it.[87] In this case, in dealing with the reasonableness of an agreed security procedure, reliance was put[88] on a guidance issued in October 2005 by the agencies of the Federal Financial Institutions Examination Council (FFIEC) and titled 'Authentication in an Internet Banking Environment' (Guidance). The Guidance explained that authentication methodologies involve three basic 'factors': '[s]omething the user *knows* (e.g., password, PIN)'; '[s]omething the user *has* (e.g., ATM card, smart card)'; and '[s]omething the user *is* (e.g., biometric characteristic, such as a fingerprint)' (original emphasis).

While not endorsing any particular technology for high-risk transactions (such as funds transfers to third parties), the Guidance disfavoured a single-factor authentication and favoured the implementation by financial institutions of 'multifactor authentication, layered security, or other controls reasonably calculated to mitigate . . . risks'.

In the facts of the case, the customer

> '. . . agreed to the core security procedures visible to users that comprised the key components of the integrated security package used by the Bank. [It] expressly agreed to the use of security passcodes, which consisted of a customer ID and customer password and a user ID and user password for each authorized user of the customer, . . . and it agreed by course of performance to the use of challenge questions, having cooperated in setting up answers to such questions and having answered them in the course of conducting eBanking.'

It also 'effectively agreed to monitor its commercial accounts daily'.[89] The agreed security procedure was strengthened by invisible elements such as risk profiling for the customer, device cookies placed onto customers' computers to identify particular computers used to access online banking, and subscription to eFraud Network.[90]

---

[86] Supra note 51 (2011).

[87] The case, in conjunction with others discussed here, is extensively examined in law reviews. See, for example, RK Burrows 'Increased bank liability for online fraud: The effect of *Patco Construction Co.* v. *People's United Bank*' (2013) 17 *North Carolina Banking Institute* 381; Salvatore Scanio and Robert W Ludwig 'Surging, swift and liable? Cybercrime and electronic payments fraud involving commercial bank accounts: who bears the loss?' (2013) 16(10) *J of Internet Law* 3; M Waite 'In search of the right balance: *Patco* lays the foundation for analyzing the commercial reasonableness of security procedures under UCC Article 4A' (2013) 54 *Boston College LR* E-Supplement 217.

[88] *Patco Constr v People's United Bank supra* note 51 (2011) at *25–*32.

[89] At *104–*106.

[90] At *34–*38.

Over a period of several days, the alleged fraudulent transfers kept raising the risk scoring. The bank posted email alerts but the customer was not vigilant in resorting to this option or in monitoring the account activity daily. With no response from the customer, the bank kept executing the payment orders, as neither incorrect password nor incorrect answer to a challenge question was submitted by the initiator.

In challenging the commercial reasonableness of the security procedure, the customer argued that the authentication procedure did not truly consist of 'layered security.' Thus, while authentication required both codes and answers to challenge questions, the effect of each stage in which enhanced risk was perceived was to trigger more challenge questions. In addition, the customer argued that over time the increased frequency with which challenge questions had been asked did not enhance security but increased risk by giving hackers greater opportunity to find out the correct answers to them. The District Court rejected these arguments and found that the authentication procedure truly consisted of 'layered security.' It held that overall, even though it was not optimal, the security procedure certainly met the commercially reasonable standard. Pointing out that in the wake of the transfers the customer failed to isolate its computer or forensically preserve the hard drives, the district court concluded that a security breach could have occurred only at the customer's end. It gave a summary judgment in the bank's favour.

It is obvious that the District Court in *Patco* interpreted 'access to transmitting facilities of the customer' in section 4A-203(*a*)(2) as including virtual access by a hacker. The case was thus resolved solely on the basis of the bank's good-faith compliance with an agreed-upon commercially reasonable security procedure, because the customer was unable to prove that its system had not been the source from which the hacker had obtained the information. True, the customer was not free of negligence and yet, according to the District Court, its existence or absence played no role in the final outcome.

The United States Court of Appeal of the First Circuit reversed the decision.[91] It first pointed out that '[a]lthough the bank's security system flagged each of these transactions as unusually "high-risk" because they were inconsistent with the timing, value, and geographic location of Patco's regular payment orders, the bank's security system did not notify its commercial customers'.[92] Specifically overruling the District Court on the effect of the increased frequency with which challenge questions had been asked and citing 'Article 4A's mandate that security procedures take into account "the circumstances of the customer" known to the bank',[93] the Court of Appeal was of the view that

> '[The bank] did substantially increase the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and high dollar transfers. Then, when it had warning that such fraud was likely occurring in a given transaction, [the bank] neither monitored that transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable. We emphasize that it was these collective failures taken as a whole, rather than any single failure, which rendered [the bank]'s security system commercially unreasonable.'[94]

Nonetheless, while finding the bank's security procedure to be commercially unreasonable, the Court of Appeal declined to give a summary judgment in Patco's favour. Recognizing the limited customer's duty under section 4A-204(*a*) 'to exercise ordinary care' in advising the

[91] *Patco Constr v People's United Bank* supra note 51 (2012).
[92] At 197.
[93] At 211–212.
[94] At 210–211.

bank of an unauthorized payment order, a duty that had not been breached by Patco, the Court of Appeal declined to treat it as setting the upper limit of the customer's duties to the exclusion of any other and observed that '[i]t is unclear, however, what if any obligations a commercial customer has when a bank security's procedure is found to be commercially unreasonable'.[95] The Court of Appeal did not rule out the application of external general principles of law in the determination of the matter. Accordingly, it left 'open for the parties to brief on remand the question of what, if any, obligations or responsibilities are imposed on a commercial customer under Article 4A even where a bank's security system is commercially unreasonable'.[96]

CONCLUSION

An authorized payment order may be enforced pursuant to section 4A-202(*a*), even without security procedures. Otherwise, article 4A requires good-faith compliance with an agreed commercially reasonable security procedure. This meets banks' expectations.

In turn, customers wish to remind banks that they are 'custodians of the customer's money' providing for 'a safe place of deposit'[97] so as to leave banks liable, even in a case in which an agreed-upon commercial reasonable security procedure has been complied with by the bank, at least as long as no fault (or even no gross negligence) has been attributed to the customer. This expectation is, however, met by article 4A only in part. An unauthorized, albeit properly verified, payment order binds the customer, unless the customer proves that the order was caused by an interloper. This is a very narrow exception that does not apply where a hacker managed to compromise the customer's security system even with no, or very little, fault on the part of the customer.[98]

In *Patco*, the Court of Appeal left 'open . . . the question of what, if any, obligations or responsibilities are imposed on a commercial customer under Article 4A even where a bank's security system is commercially unreasonable'.[99] Thereby the court appears to exceed banks' reasonable expectations and to increase commercial customers' frustration. Not only are commercial customers not allowed to defend themselves against a non-negligent bank by proving that they were also not negligent, but they may lose out even where the bank was in fact negligent, because of some (as yet unspecified) duties not even found in article 4A.

---

[95] At 214–215.

[96] Ibid.

[97] *National Bank of Virginia v Nolting* supra note 5.

[98] By comparison, under the Cambodia Law on Negotiable Instruments and Payment Transactions, 2005, NS/RKM/1005/030, '. . . the person identified as sender on the payment order is not liable, when the person proves . . . that the issue of the unauthorized payment . . . order was not caused by: (i) The person identified as sender, or someone entrusted at any time with duties to act for that person with respect to payment transactions or the security procedure; or (ii) Someone who obtained from the person identified as sender, or a source controlled by that person, access to that person's transmitting facilities, or information, including any access device, computer software, or the like, facilitating breach of the security procedure.' As well, under art 214(4) of the same statute, '[a] sender of a payment order . . . shall exercise ordinary care in order to prevent forgery and unauthorized issue or alteration of payment orders'. While modelled on UCC s 4A-203(*a*)(2), art 213(2) in Cambodia is less 'demanding' of the customer, and in conjunction with art 214(4), is to be read as meaning that absent breach of trust or negligence, a customer will not be liable for an unauthorized payment order. See Benjamin Geva 'Payment system modernization and law reform in developing nations: lessons from Cambodia and Sri Lanka' (2009) 126 *Banking LJ* 402 at 418–419. The statute can be accessed at http://www.nbc.org.kh/download_files/legislation/others_law_eng/ law_on_negotiable.pdf (accessed 18 November 2013).

[99] *Patco Constr v People's United Bank* supra note 51 (2012) at 48.

In the final analysis, in attempting to provide for a fair balance between banks and customers in the allocation of unauthorized and yet properly verified wire payment order losses, the scheme under article 4A is a great leap forward. However, statutory language must be improved and courts' awareness of pertinent policy considerations increased. This is not only in order to eliminate a few uncertainties[100] but also to fine-tune the overall loss allocation scheme so as to establish a better balance between the legitimate expectations and interests of relevant parties.

[100] Drafting deficiencies are set out in the text to footnotes 79–82.