Funds Transfers under UCC Article 4A: What is a Commercially Reasonable Security System?

By Stuart R. Hene

[Ed. note: The Oklahoma Bar Association (OBA) Financial Institutions and Commercial Law Section, through its Legislative Review Subcommittee, reviews prospective legislation in Oklahoma to assess and better assure its fit into other, related Oklahoma law. The Section also participates in writing, in conjunction with the OBA Uniform Laws Committee, reports on new legislation and “Oklahoma Comments” for publication in the Oklahoma Statutes Annotated, once the legislation passes, to explain the impact of the bill on Oklahoma law and cases. See, e.g., Fred H. Miller & Alvin C. Harrell, The Work of the Oklahoma Bar Uniform Laws Committee: Oklahoma Enacts UCC Article 3 and 4 and 4A Amendments, 63 Consumer Fin. L.Q. Rep. 29 (2009).

The members of the Section are among Oklahoma’s top specialists in the field. To encourage new, and younger, members, the Section also sponsors a writing contest for law students at Oklahoma law schools. This article is derived from a paper that won article 3 and 4A Amendments.

I. Introduction

Suppose you are the owner of a multi-million dollar construction company and you want to obtain a new fleet of construction equipment vehicles. The sales price and other terms of the sales contract have been duly negotiated. Financing has been arranged (as needed), and now it is time for the sale to be completed. This means it is time to transmit the payment for the vehicles and equipment. At that moment the buyer and seller face a choice among alternative payment systems. The seller wants to receive the equivalent of cash, but obviously coin and currency are not practical in these circumstances. Instead, a transfer of funds between two bank accounts and probably two different banks will be needed. Among the basic alternatives are: (1) the use of a negotiable instrument governed by Uniform Commercial Code (UCC) Articles 3 and 4; or (2) a funds transfer governed by UCC Article 4A. Today, the option chosen is increasingly likely to be the latter. This article analyzes the security system needs that should be considered in order to ensure a safe and non-fraudulent transfer of the funds from one bank to another under Article 4A.

Article 4A funds transfers may be originated in numerous ways; e.g., a telephone call, a facsimile (FAX) message, or an internet transfer.1 Many of these transfers are now originated over the internet, and at the core of this information infrastructure is cyberspace:2

Cyberspace is [the] nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.3

1. See UCC Article 4A § 4A-103(a)(1), and id. § 4A-104, Official Comments 5 and 6. Section numbers cited herein reference UCC Article 4A unless otherwise noted.
3. Id. at vii.
Because of the vast reliance on cyberspace for commerce in modern society, security in the transmission of financial information is a critical legal issue. In many cases, "all of a company’s daily transactions and all of its key records are created, used, communicated, and stored in electronic form using networked computer technology." Electronic communication of such information is also essential to the functioning of electronic payment systems. A payment system "is a system that is used to transfer value from one person to another in order to pay for goods, services, real estate, or other desired items. A functioning payment system is a necessary component of economic development," as well as individual transactions.

A primary example of a modern, functioning electronic payment system is the Article 4A funds transfer. Such transfers can be used for multiple purposes and are commonly relied on in commercial transactions. "A funds transfer should not be confused with a 'money transfer.'" [That is ] where currency is exchanged from one person to another. Instead, a funds transfer is the transfer of bank credit.

During a funds transfer, each bank must make decisions with regard to a series of events within a short period of time. Issues that each bank must consider include: whether the payment is an authentic order; whether there are any errors in the check for payment or furnishing other evidence of authority to cause an account to be debited.

The Article 4A funds transfer system has made it faster and easier for individuals and companies to quickly and safely transfer large dollar amounts to a beneficiary’s account. However, a funds transfer still poses multiple potential risks to the parties involved in a payment transaction.

These risks include, but are not limited to: a credit risk; a risk of electronic failures during the transactions; a risk that mistakes could be made during the transactions; the risk of costs exceeding the efficiency of the transactions; and a fraud risk. This article focuses on the latter risk—the risk of fraudulent transfers.

A risk of fraud can arise when a "purported payor does not actually have the right to push value from the account in a particular transaction or where the payee does not actually have the right to pull value from the debit account." For example:

If recovery is unavailable for some reason against the wrongdoer, then one of the parties to the payment transaction will bear that risk, even if that party acted innocently and with all due care. The risk of this type of fraud could rest on the payee, the payee’s bank, the purported payor, or the payor bank.

The risk of a fraudulent transfer remains one of the greatest risks for parties engaged in payment transactions. In an effort to address the risks of unauthorized access and use, various laws and regulations have been enacted or issued. However, “[m]any transactions in which the payor’s instruction to its bank is made through some mechanism other than a check are governed by UCC Article 4A, or [related] funds-transfer system rules.

II. EFTA and the UCC

A. Scope of the EFTA

The Electronic Funds Transfer Act of 1978 (EFTA) governs electronic funds transfers to or from a consumer account. The EFTA is implemented by Regulation E, as promulgated by the Federal Reserve Board (FRB). The FRB also prepares and updates an Official Staff Commentary to Regulation E (the Commentary).

This Commentary provides essential guidance on application of the complex requirements set forth in Regulation E.
the EFTA. Specifically, the EFTA defines an electronic fund transfer as:

any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account. Such term includes, but is not limited to, point-of-sale transfers, automated teller machine transactions, direct deposits or withdrawals of funds, and transfers initiated by telephone.

Because such transfers are excluded from Article 4A, this EFTA definition is important to the scope of Article 4A. There are two principal requirements in this definition of electronic fund transfer, as specified in the EFTA, regarding an authorized electronic funds transfer. First, the transaction must debit or credit an ‘account.’ Second, there must be a transfer of funds initiated by the specified electronic means.

This may sound similar to the Article 4A concept of a “payment order,” as defined at section 4A-103. However, the EFTA is essentially limited to “retail” funds transfers by consumers.

The EFTA defines an unauthorized electronic fund transfer as “an electronic fund transfer from a consumer’s account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit…”

However, this definition of an unauthorized electronic funds transfer does not include: (1) transfers initiated by the consumer with fraudulent intent or any person acting together with the consumer; (2) a transfer initiated by anyone who was given any means of access to the consumer’s account; or (3) a transfer in which there occurred an error on behalf of the bank. So, what happens under the EFTA if a fraudulent transfer does occur? In such a case, the burden of proof lies with the bank to prove that the electronic fund transfer was either authorized by the consumer or, if unauthorized, meets the requirements for consumer liability. If it was unauthorized, the bank will be liable for a failure to follow the terms and conditions of the account in regards to the electronic funds transfer.

B. Scope of Article 4A

In comparison with the EFTA (which is limited largely to error resolution and the allocation of liability for losses), UCC Article 4A governs the basic elements of an electronic fund transfer. However, as noted, Article 4A does not apply to a “retail” funds transfer that is governed by the EFTA. In contrast, Article 4A governs: (1) FedWire; (2) CHIPS; (3) SWIFT; or (4) telex; and (5) book transfers, which are simply transfers of credit across a single bank’s books from one account to another. Thus, a fundamental distinction is that “retail” EFTA transactions are governed by private (e.g., contractual) funds transfer rules and the EFTA dispute resolution rules, while Article 4A governs both the basic transactional elements and the error or fraud resolution issues in a “wholesale” Article 4A funds transfer (while being supplemented to some extent by contractual and private rules).

As suggested above, Article 4A funds transfer transactions are commonly referred to as a “wire transfer” or a “wholesale funds transfer.” The term ‘wholesale’ distinguishes the Article 4A funds transfer from a ‘retail’ consumer electronic funds transfer governed by Regulation E and the EFTA.

Article 4A defines the basic elements of a funds transfer, as a series of offsetting transactions which begins with an originator’s payment order and concludes with payment to the beneficiary of that order.

C. Addressing Fraud Risk

All payment systems have to contend with the risk of fraud, which in the case of commercial payment orders under Article 4A can be for very large amounts. Addressing this problem is critical to the usefulness of the Article 4A payment system. Therefore, in an effort to address and curtail fraudulent transfers, Article 4A includes a carefully-crafted commercially reasonable security procedure provision.

Article 4A requires a payment order to be authorized in order for the funds transfer to take place. “A payment order received by the receiving bank is the authorized order of the person identified as the sender if that person authorized the order or is otherwise bound by it under the law of agency.” Thus, a funds transfer will be effective whether or not the order is authorized if the originator is obligated under the rules governing vicarious or apparent authority. Often this will depend on whether the originator’s bank and the originator have agreed on verification security procedures. “[T]he security procedure [must be]
a commercially reasonable method of providing security against unauthorized payment orders, and...the bank [must prove] that it accepted the payment order in good faith and in compliance with the security procedure.”

A security procedure is established by agreement between the customer and the bank, in order to verify that a payment order is properly placed and is that customer’s payment order, and to detect errors in transmissions of payment orders. A crucial point is the commercial reasonableness of the security procedure.

D. Commercial Reasonableness

Commercial reasonableness is a question of law. There are several factors in determining whether a security procedure is commercially reasonable. Article 4A specifies certain factors that a court is to consider, namely whether:

(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.

Along with these two factors, a court may consider: whether the wishes of the customer were expressed to the bank; whether the circumstances of the customer were known to the bank, “including the size, type, and frequency of payment orders normally issued by the customer to the bank;” whether alternative security procedures were offered to the customer; and the security procedures in use by other banks in similar situations.

The foundational rule is that a bank is liable for any unauthorized payment it makes. However, it is the customer and not the bank who is liable for the loss if a commercially reasonable security system, agreed to by the customer, was in place, and the bank complied with it. Also, the customer is liable if the customer fails to notify the bank within one year of a fraudulent or erroneous electronic funds transaction. However, the bank can be liable for the loss if it agrees in writing to be liable for part of the loss or if the bank and customer agreed to a security procedure that was not commercially reasonable. In addition, “if the customer is able to establish that an unauthorized but effective order was not attributable to any responsible person entrusted to act for the customer or any access obtained from the customer’s side,” then the bank will be liable for the loss. These limits on the customer’s liability reflect a basic tenet that the bank is obligated to take reasonable steps to guard against fraud, critical risks, and security threats.

Article 4A does not establish the specific parameters of a security procedure that will be accepted among the courts, recognizing that this is a matter for the development of commercial practice. However, Article 4A does state that “[a] security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices.”

However, just because a bank uses one of these permissive approaches does not mean that a court will find that the bank had a commercially reasonable security system in place, or that another bank was unreasonable in using another approach. A commercially reasonable security procedure could utilize all of the elements, a portion of the elements, or entirely different techniques than those described in section 4A-201. In order to facilitate the development of commercial practice, Article 4A leaves courts to consider, as a question of law, whether the procedures in place in a given case constitute a reasonable security procedure as adapted to the specific situation.

III. The Courts’ Determinations of Commercially Reasonable Standards

A. Introduction

Reflecting this flexibility, the courts have not specified a single standard for determining whether a security system is commercially reasonable. In one instance a court may employ a specific set of factors; in another instance, the same court may recognize a different approach. Also, commercially reasonable security procedures may employ variations of different techniques in different combinations. One thing that is clear, however, is that determining whether a security system is commercially reasonable is a question of law. Therefore, the courts must review each scenario on a case-by-case basis to determine if the security procedure in question is commercially reasonable in that context, and the other requirements for a recovery have been met.

For example, in Covina 2000 Ventures Corp. v. Merrill Lynch, Pierce, Fenner & Smith, Inc., the court applied Article 4A’s foundational rule, which states that a bank will bear the loss of any unauthorized funds transfer. The court noted that the rule is subject to an “exception when the bank and the customer agree on a ‘security procedure’ to ensure that payment orders received by the bank are

42. Id.
43. See § 4A-201.
44. See § 4A-202(c).
45. Id.
46. See Miller, supra note 37, at 20 (citing § 4A-505).
47. Id. (citing § 4A-203).
48. Id.
49. Id.
50. See § 4A-201.
51. See § 4A-203, Official Comments 3 and 4.
52. See § 4A-201 - 4A-203, and Official Comments thereto.
54. See, e.g., id, and discussion below.
56. Id. at *1 (see also UCC Article 4 § 4-203, Official Comment 1, and Article 4 Prefatory Note).
authorized."57 In Covina, Mr. Ma opened a corporate account at Merrill Lynch for two different companies.58 One of these companies was Covina 2000 Ventures Corporation. Between the months of June 2002 and April 2004, $9 million was transferred out of these accounts.59

Merrill Lynch and Mr. Ma did not have an agreement referring to the security procedure necessary to authenticate a funds transfer.60 Twenty-one of the letters of authorization for the wire transfers contained a notation indicating confirmation from Mr. Ma and twenty-four of these authorizations also contained an apparent signature by Mr. Ma.61

In Covina, Merrill Lynch (the bank) did not argue the issue of a commercially reasonable security procedure because the bank argued that the customer (the plaintiffs) were liable for the funds transfer on agency grounds. The bank also argued that the suit was brought more than four years after the fraudulent transfers occurred, contrary to the one-year requirement.62 The Covina court decided the case based on the latter requirement, i.e., that a customer of a bank cannot bring a claim for a fraudulent Article 4A transfer after one year.63 Thus, Covina does little to define what constitutes a reasonable security procedure. On this issue, the court merely stated: "[O]nly when a commercially reasonable security procedure is in place (or has been offered to the customer) may the bank disclaim its liability for unauthorized transfers."64

B. The Regatos Case

In Regatos v. North Fork Bank,65 the court took a further step in articulating what constitutes a commercially reasonable security system. In Regatos, the plaintiff (Mr. Regatos) had opened an account with the Commercial Bank of New York (the bank). When Mr. Regatos opened this account he signed an Account Information form. This agreement stated that Mr. Regatos was allowed to make wire transfers out of his account via payment orders, transmitted from his home in Brazil.66 There was a specific procedure to be followed each time by the bank and Mr. Regatos to ensure valid transfers. First, Mr. Regatos would sign a payment order which would be faxed to the bank.67 Next, a confirmatory phone call would either be placed by Mr. Regatos to Ms. Abadi, a bank employee, or to Mr. Regatos from Ms. Abadi.68 After the confirmation of the amount, Ms. Abadi would FAX the payment order to New York where signature confirmation would take place by comparing the payment order and the signature on record.69 However, this security procedure lacked a password or algorithm element of identification.70 During the spring of 2001, two funds transfers were initiated from Mr. Ragatos account, both of which Mr. Ragatos claimed he did not authorize or initiate.71

The Regatos court applied the foundational rule of Article 4A, as in Covina: That is, foundationally, "the bank will bear the loss of any unauthorized funds transfer."72 However, the Regatos court noted that an exception to this rule is triggered when the bank and the customer agree to a security procedure that is commercially reasonable.73

A payment order accepted in good faith pursuant to a commercially reasonable security procedure is said to be "effective" as the order of the customer because it can be properly verified. Such an order is effective even if it is actually unauthorized, as in the case of a perfect forgery. But where a payment order is not effective—or where a payment order is unauthorized and there is no security procedure in place the bank has an invariable duty to refund the lost funds.74

Therefore, the Regatos court noted that it had to decide whether there was a commercially reasonable security procedure in effect. For every funds transfer, the bank and Mr. Regatos adhered to the same procedure.75 The court "[f]ound the security procedure followed by the Sao Paulo office, coupled with the signature comparison done at the New York office, to be commercially reasonable."76 The court specifically concluded that, although comparison of a signature alone is not sufficient, with the other elements coupled to this procedure it was acceptable.77 The three-step process of a signed order, confirmatory phone call, and signature comparison was sufficient to constitute a commercially reasonable security procedure.78 Although the three-step procedure lacked recorded conversations and passwords or algorithms, the confirmatory phone call to or from the same pre-identified bank representative ensured a commercially reasonable procedure.79

87. Id.
88. See id.
89. See id.
90. See id.
91. See id.
92. See § 4A-505.
94. Id. at *6 (quoting Regatos, 5 N.Y.3d at 403, discussed infra).
95. Id.
97. See id. at 636.
98. Id.
99. Id.
100. Id.
101. Id.
102. Id.
103. See Regatos, 257 F. Supp. 2d at 636.
104. Id. at 641 (citing N.Y. UCC §§ 4-A-202(2), 4-A-203).
105. See id. at 646.
106. Id. (citing N.Y. UCC § 4-A-201).
107. See id.
108. Id.
109. Id.
C. The Braga Case

Applying the standards articulated in Regatos, the court in Braga Filho v. Interaudi Bank set forth an additional example of commercial reasonableness. In Braga Filho, the plaintiff (Braga) opened an account at the Interaudi Bank in New York City (the bank) while visiting New York on a trip from his home in Brazil. When the account was opened, Braga signed a Telecommunications Authorization agreement (the agreement). The agreement provided “that the Bank was authorized ‘to accept and immediately act upon instructions from [the customer] via telephone, telegram, telefacsimile, untested telex, electronic mail, or any other means of telecommunications.’” The agreement also provided “that the Bank would ‘select security procedures for accepting instructions that are commercially reasonable for [the bank].’” The security procedures that the bank would adhere to were printed on an internal document not available to the bank’s customers, entitled “Funds Transfer Policy and Procedures.” This document contained instructions and procedures to which the bank’s staff was supposed to adhere.

For all funds transfer requests (i.e., payment orders), the bank would verify the customer’s signature on file with the signature on the payment order, confirm that the account contained sufficient funds, obtain approval from an account officer, and then forward the payment order to the bank’s Paying and Receiving Department. In addition, for requests made by email or fax, there were special guidelines. These guidelines stated that the customer had to be called before the request would be forwarded to the Paying and Receiving Department; the customer had to answer security questions when contacted, and the confirmation contact call was to be recorded. Two years after the account was opened, nearly one million dollars was transferred out of the account, unbeknownst to the plaintiff/customer (Braga). These fund transfers were based on payment orders in the form of fax requests, and Braga later claimed there was no confirmation telephone call for verification. Braga contacted the bank upon realizing that the money was no longer in his account. The woman with whom he spoke at the bank informed Braga that she had spoken with Braga several times and therefore knew that he was not Braga (even though he was Braga).

Braga then brought an action to recover the funds from the fraudulent transfer. The court noted “that when a customer has agreed to a bank’s security procedure, the customer will bear the risk of loss if the security procedure was ‘commercially reasonable’ and if the bank followed that procedure.” The court then conducted an analysis based on that set forth in Regatos. The Braga court focused on the fact that the parties agreed to a three-part security procedure which consisted of a signed order, confirmation phone call, and a signature comparison. The court again noted that a signature comparison alone is not sufficient to establish commercial reasonableness. However, because the signature comparison was coupled with the other two elements, the Braga court found the procedure in that case to be commercially reasonable. In applying the holding from Regatos, the Braga court reasoned that:

1. See id. at *2.
2. See id. at *3.
3. See id.
4. See id. at *5.
5. See id. (citing N.Y. UCC § 4A-202(2)).
7. See id. (citing N.Y. UCC § 4A-201).
used in Regatos.” So, the confirmation telephone call, an answer to security questions during that confirmatory phone call, and a recording of the confirmatory phone call constituted a valid and commercially reasonable security procedure.

D. The Centre-Point Case

In Centre-Point Merchant Bank LTD v. American Express Bank LTD, the court adopted a more specific two-part analysis in determining whether the bank’s actions and procedures were commercially reasonable. Centre-Point, a Nigerian Bank, and American Express Bank LTD (AEBL), entered into a banking relationship. The two banks communicated by telex and used a telegraphic key code to conduct all transactions. Four years after the account was opened, Centre-Point telexed AEBL to debit a large sum from the account and invest that sum in a fixed deposit. The following day, AEBL replied via telex advising on the interest rate; however, Centre-Point never received this telex. “Instead, [Centre-Point] received an altered telex confirming that AEBL had followed its instructions and debited the account.”

At the same time, AEBL received a cancellation telex from Centre-Point. AEBL then implemented the security procedure and applied the test key code, and this indicated that the key code was valid. Unbeknownst to any of the parties involved, a Centre-Point employee had altered the telexes that each bank received. Therefore, neither bank was aware of the fraudulent payment orders, or non-orders. Because the telexes received were not the telexes sent by the banks, Centre-Point argued that a lack of a commercially reasonable security procedure existed in the transaction and was responsible for the loss.

The Centre-Point court, applying Article 4A, adopted a two-part inquiry. The first part of the inquiry was whether the particular security procedure was commercially reasonable, and the second part of the inquiry was whether AEBL complied with the procedure. In applying this two-part inquiry, the court adopted a more definitive standard than those applied in Covina, Regatos and Braga. When determining whether or not a security system is commercially reasonable, the Centre-Point court held that: “[t]he 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.” For example, if both parties agreed on a procedure designed to eliminate fraud and adopted a security system to protect each party’s interests, it is likely to be commercially reasonable. Therefore, “[a] security procedure is not [going to be] 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.”

Furthermore, to answer the question of commercial reasonableness, the court said it would analyze security procedures in place in similar situations between similar parties. Critiquing the system used by AEBL with the standard adopted, the Centre-Point court determined that the telex test key code was a commercially reasonable security system. Centre-Point admitted that it never objected to the security procedure in place, and Centre-Point also admitted that all banks in Nigeria used essentially the same security procedure. In addressing the second part of the inquiry as set forth by the court, AEBL also confirmed that all test key codes received were tested properly and confirmed. Therefore, because AEBL received a valid test code, even though the codes were not legitimate, AEBL sufficiently complied with the security procedure agreed upon by both parties. Because the test key code was commonly used by all similar banks in the area and there was valid compliance, the court found “that the telegraphic test key [met] the ‘commercially reasonable’ standard required by the statute.”

E. The Grabowski Case

In contrast to the Regatos, Braga, and Centre-Point cases, Grabowski v. Bank of Boston illustrates an instance in which a commercially reasonable security system was not present. In Grabowski, the plaintiffs entered into various agreements with the Kinder Company (Kinder), which operated an investment program for buying and selling prime commercial debt instruments and securities. Kinder proposed that the plaintiffs open the accounts at the Bank of Boston (the Bank) and execute powers of attorney granting Epstein, the principal for Kinder, control over the accounts. “Kinder’s agents told the plaintiffs [that] this power of attorney would protect their funds and the account would hold cash and securities,
which the Bank would authenticate.”\textsuperscript{121} Funds were eventually transferred into the accounts and, simultaneously, Epstein directed the bank to execute funds transfers from these accounts.\textsuperscript{122}

While directing the Bank to withdraw funds from the accounts, Epstein failed to replace “the funds with an equivalent amount of prime bank instruments or in-voices,”\textsuperscript{123} as the agreement between the plaintiffs and Kinder required. Defending the commercial reasonableness of its security procedure, the Bank argued that it was not liable for the funds transfers. Although the court found that the Bank was not liable (because the transfers were authorized), the court also determined that there was no commercially reasonable security procedure in place.

Article 4A eliminates the liability of a bank if the customer and the bank have agreed to a security procedure for verifying the authenticity of any transfers.\textsuperscript{124} The Grabowski court concluded that: “\textsuperscript{125}The Commercial Deposit Account Resolution [Account Resolution] relied on by the Bank here is not an enforceable modification of the loss allocation scheme set forth in Article 4A.”\textsuperscript{126}

The Account Resolution was not an enforceable modification because it contained only “a general modification of liability under Article 4A without an accompanying commercially reasonable security procedure.”\textsuperscript{127} No security procedures, such as verification callbacks, recordings of the call, or secure passwords existed in the Commercial Deposit Account Resolution.\textsuperscript{128} Instead, the Account Resolution provided only an indemnity provision.\textsuperscript{129} Therefore, “because the Account Resolution [purports to be] a modification of the baseline loss allocation scheme of [A]rticle 4A and not an agreement on a security procedure, the general indemnity provision relating to unauthorized payment orders is unenforceable under . . . [A]rticle 4A.”\textsuperscript{120}

The Grabowski case makes clear that an indemnity provision in a deposit account agreement, alone, will not suffice to establish a commercially reasonable security procedure. In the final analysis, an agreement between the bank and the customer needs to be reached, regarding not only an indemnification provision but a commercially reasonable security procedure as well. At a minimum, features like the procedures upheld in Regatos and Braga should be considered.

\section*{IV. So Exactly What is Commercially Reasonable?}

\subsection*{A. Introduction}

As noted, there is no precise definition or rule that lays out specific requirements for a commercially reasonable security procedure.\textsuperscript{130} On one hand, a commercially reasonable security procedure might include several procedures lumped together to create a commercially reasonable system.\textsuperscript{131} On the other hand, a commercially reasonable security procedure could consist of one specific procedure that is considered commercially adequate.\textsuperscript{132} However, there is a growing trend concerning certain practices and techniques that seem to be developing as an industry standard and custom for what constitutes a commercially reasonable security procedure. Many businesses, in addition to banks, are operating online banking and funds transfers systems, effectively operating the business in cyberspace, and are implementing security procedures for these transactions.

\subsection*{B. Wheatman Recommendations}

Many of these companies, including banks and other financial institutions, are adopting innovative procedures and policies to ensure that they are complying with the requirements for a commercially reasonable security procedure. For instance, Vic Wheatman with the Gartner Company, a provider of market research covering the information technology industry, has explained eight steps that he believes are needed to define a commercially reasonable security system.

First, “[o]rganizations need to examine the status of commercially available computer technology and, specifically, information security technology.”\textsuperscript{133} In this stage, banks and other financial institutions need to be made aware of the fact that there are different systems to protect different types of information. Of course, the larger and more complex the financial institution, the more extensive and complex the system needed.

Secondly, “[o]rganizations always need to assess the affordability of security technologies, procedures and techniques.”\textsuperscript{134} Because larger and more complex financial institutions will need larger and more complex systems, these systems will cost considerably more than smaller systems. Small institutions and small businesses need to carefully weigh the costs against the potential loss from fraudulent transfers and hackings before expanding into areas of operation that will require implementing the most expensive security system.

Third, “[g]iven the growing list of failures in systems, the likelihood of a technological security failure should be considered fairly high.”\textsuperscript{135} Technology is not perfect and is always subject to glitches and malfunctions. Therefore, backup

\begin{thebibliography}{99}
\bibitem{121} Id.
\bibitem{122} See id. at 117.
\bibitem{123} Id.
\bibitem{124} See id. at 120 (and UCC Article 4A §§ 4A-201, 4A-202, and 4A-203).
\bibitem{125} Id.
\bibitem{126} Id.
\bibitem{127} See id.
\bibitem{128} See id. at 116.
\bibitem{129} Id. at 120.
\bibitem{130} See supra Part II.D.
\bibitem{131} Id.; see also supra Parts III.B.-E.
\bibitem{132} Id.
\bibitem{133} Vic Wheatman, Management Update: Eight Steps Needed to Define Reasonable Security, June 8, 2005, available at http://www.solutions-mag.com/Data/Newsletters/CSWPS.266\textsuperscript{26}0\textsuperscript{26}Gartner\textsuperscript{26}Alleges\textsuperscript{26}To\textsuperscript{26}Security\textsuperscript{26}Out (last visited Feb. 2, 2009).
\bibitem{134} Id.
\bibitem{135} Id.
\end{thebibliography}
systems and manual systems need to be in place to ensure the authenticity and validity of transfers and to decrease the chances of fraudulent transfers occurring.

Fourth, an institution must consider the harm that can result from a security failure.136 The potential harm to consider has at least two fronts. One is the potential harm to a customer whose private information could be leaked on the internet or who could be the victim of a fraudulent transfer.137 The other potential harm is the risk to the bank in a situation where there is a breach or fraudulent transfer. The financial institution could be subject to liability for the amount of the transfer or for penalties assessed on it by a court or a state or federal government.138

Fifth, financial institutions and companies need to anticipate security threats.139 Obviously the internet is not always a safe environment. Hackers are always trying to get into secure systems. Furthermore, dishonest employees must be kept at bay and not tempted to steal personal information or induce fraudulent transfers.

Sixth, “[r]easonable security in the absence of widely accepted standards is difficult.”140 There isn’t a single security system that is the best or is the most commercially reasonable security system in all contexts. Different procedures, systems, and techniques may work differently in different situations. A key solution is to look to the industry custom or at what other financial institutions in the market are using as their commercially reasonable security procedure.

Seventh, an organization should look at the best practices on the market.141 “An organization should at least do what its peers are doing.”142 Finally, Wheatman recommends that a financial institution or company implement routine audits.143 Security systems and technology are always changing. As noted, hackers are always finding ways around current security systems. Furthermore, new systems are being developed each day. “Self-assessment is a useful information-gathering technique that can help determine the degree to which a chosen standard is being met….144 Wheatman emphasizes that having the right managerial procedures in place makes it more likely that a commercially reasonable security system will be implemented and maintained.

C. Password Systems

Currently, the most commonly used security system for online transactions requires a complex password containing more than six keys and at least one number. As noted below, however, over the past few years at least two major internet sites have been compromised, revealing all related passwords. Although neither of the sites involved commercial transactions, many other sites are following their lead in changing their password requirements.

In 2007, the social networking site of Myspace was compromised. This “hacking” revealed 30,000 passwords and usernames.145 More recently, the site of phpbb.com was compromised revealing 20,000 passwords.146 Following the hacking of this site, a study of the type of passwords chosen was conducted by Robert Graham.147 Graham determined that the common approach, as to how people choose their password, is to use an ordinary, easily identified password if there were no password requirements. Among the leading choices were people’s first names, patterns on the keyboard, or variations of the word “password.”148 Using a password that matches the user’s first name constitutes zero security protection. A password in the form of the user’s first name is just the username typed a second time. The user’s name appears on the screen and the hacker doesn’t even have to guess.

Similarly, people’s choices of patterns on the keyboard often provide zero security protection. Common choices for keyboard sequences include: “1234,” “qwerty,” or “asdf.”149 Again, this takes the probability of having a safe password out of the equation. A hacker can easily access any personal or financial information if a user employs a password of this sort. Therefore, “[t]he widely-deployed use[s] of user ID/password protection schemes are no longer considered adequate protection for online information. Though user ID/PIN/password are still the most common solution for online authentication, there is significant interest in replacing passwords with more robust multifactor authentication.”150

D. Other Procedural Safeguards

Although the use of user identification (ID), personal identification numbers (PIN’s), and similar passwords is commercially reasonable under UCC Article 4A,151 there is a trend toward adoption of more secure methods of commercially reasonable security procedures in the banking industry, at least for large or sophisticated transactions. For example, it has been recommended, in the use of a call-back procedure to verify authentication, that three different employees be used, in order to reduce the opportunities for fraud.152 “One…employee receives the information and prepares the transfer
instructions; [o]ne...employee validates (determines that the information exists) and verifies (tests the truthfulness or accuracy of the information); and [o]ne...employee sends the transfer order.”

Obviously, when more eyes are used to ensure authenticity, it is harder for an invalid transfer or fraudulent intent to go unnoticed. But, importantly, no matter how many employees are involved, the receiving employee must verify the identity of the customer to ensure the authenticity of the customer placing the order transfer. The receiving employee should confirm the bank account number, PIN, and signature of the customer with the payment order being received. Also, the receiving employee, when documenting the payment order, should verify additional security information such as Social Security number, driver’s license number, signature comparison, photo comparison, and/or notarized statements. The bank will have a better chance of ensuring a valid funds transfer for each additional security check or authentication implemented.

Next, the verification employee should institute the security safeguard of a call-back. In this call-back, the verification employee double-checks important information with the customer placing the order. The verification employee will ask questions regarding the amount of the funds transfer, the destination of the transfer, the security code provided by the bank to the customer placing the order, and/or the destination account number.

Finally, the third employee, the sending employee, will verify all of the documentation filled out by the previous two employees and then will execute the payment order.

In this system, instead of one employee or one pair of eyes implementing the entire security procedure, there are three different employees verifying various aspects of the customer’s security information and payment order before the order is accepted and executed. Although this process might be time-consuming, and not suitable for every type of transaction, the liability risks of the bank should be reduced.

### E. Encryption

The use of encryption or encoding in user authentication ensures extra security in the funds transfer. Encryption “protects data from unauthorized disclosure [and] is a process in which the data is ‘scrambled or coded’ before it passes through the network.” This process uses a series of mathematical formulas and steps to transform sensitive data into a secured, encrypted form. Many banks have now adopted the American National Standards Institute (ANSI) and the International Standards Organization (ISO) standards of encryption. The “American National Standards Institute sets standards for the banking industry [and the] International Standards Organization...sets international standards.”

The standards set by these institutions include various types of data encryption protections. For example, a bank could use data encryption, user authentication, message authentication, or key management secret. Large banks and financial institutions commonly use the ANSI X9.17 standard which consists of the key management secret. “With the rapid adoption of...[these] systems by many banks across the U.S., a standard for commercially reasonable security is emerging.” The adoption of data encryption, in addition to other security procedures commonly in place, decreases the likelihood of a fraudulent funds transfer taking place. Therefore, some large banks and other institutions are implementing data encryption systems in addition to the use of passwords, user names, and PINs.

### F. Summary: Procedural Safeguards

Nothing is fail-safe; however, the more procedures the bank implements, the greater the likelihood the security procedure will be considered commercially reasonable. Security call-back procedures, recorded calls, multiple employees screening the funds transfer request and payment order, password/PIN/user name, and data encryption, in some combination coupled together, will greatly increase the odds of the security procedure satisfying the commercial reasonableness requirement of UCC Article 4A, compared to any similar feature standing alone. It should be emphasized again, however, that the law does not require any specific procedure or feature in a given context.

### V. Conclusion

Because a commercially reasonable security procedure can employ one or more of several different types of security techniques, it is best to craft a commercially reasonable security procedure “that corresponds to commonly accepted commercial practices among commonly situated Originators conducting similar types of transactions.” Therefore, other things being equal in a specific instance, the bank or other company should employ security procedures that are equivalent to what other similarly-situated financial institutions or companies are doing.

In addition, although the use of a password, PIN, or user name is still the most common form of cyberspace security, other, multifactor authentication
systems are increasingly being utilized in sophisticated transactions. 166 These systems may include the use of a verification of customer identity by various means, including the use of a customer computer, customer voice or fingerprint verification, and customer geo-location verification. 167

It should be emphasized again that the laws governing commercially reasonable security procedures can only be used as guidelines. 168 Commercially reasonable security procedures have not been specifically limited or defined in the law. This is an appropriate approach because:

[f]irst, prescribing solutions for all cases is impossible, since the circumstances are so varied that no law could begin to anticipate them all. Second, [information technology] changes so fast that what is an adequate solution today could be antiquated in just a year or two. Further, because the threat environment is changing, any definition of “good enough” is only temporary. Specificity has deliberately been left out of most regulations to accommodate such factors. 169

Thus, a standard for determining exactly what constitutes a commercially reasonable security procedure has not been clearly established by the courts or the industry. However, most financial institutions and other companies take reasonable measures to protect themselves and their customers against fraudulent funds transfers. “Banks literally spend hundreds of thousands of dollars on their security systems, and as between [the customer] and the bank, it is almost always the case that it was the customer’s system which was hacked….” 170 A good strategy entails balancing the costs generated by alternative security procedures against the intensity of the security needed. 171

In determining an appropriate approach, one should endeavor to ensure that the security procedure meets the prevailing banking standards and industry customs. If the security procedure meets prevailing industry standards, the system will have a greater chance of being held to comply with the commercially reasonable requirements of UCC Article 4A.

---

166. See id.
167. See id.
168. See, e.g., Wheatman, supra note 133.
169. Id.

---

Clarifications to Interim Rule...

(Continued from page 403)

D. Disclosures for Negative Amortization Mortgages

With respect to a negative amortization mortgage, 15 the creditor must disclose the following items:

• the interest rate at consummation and, if it will adjust after consummation, the length of time until it will adjust, and the label “introductory” or “intro”;

• the maximum interest rate that could apply when the consumer must begin making fully amortizing payments under the terms of the legal obligation;

• if the minimum required payment will increase before the consumer must begin making fully amortizing payments, the maximum interest rate that could apply at the time of the first payment increase and the date the increase is scheduled to occur; and

• if a second increase in the minimum required payment may occur before the consumer must begin making fully amortizing payments, the maximum interest rate that could apply at the time of the second payment increase and the date the increase is scheduled to occur.

The Commentary notes that the creditor must assume that interest rates rise as quickly as possible after consummation, in accordance with any interest rate caps under the legal obligation. For

(Continued on page 330)