WHAT IS A COMMERCIALLY REASONABLE SECURITY PROCEDURE UNDER ARTICLE 4A OF THE UNIFORM COMMERCIAL CODE?

C. David Hailey

I. INTRODUCTION

Every minute of every day, cybercriminals are at work. The criminal might be looking for confidential personal information that can be used for identity theft or other criminal activity. Other times the criminal might be trying to gain access to a company's online banking information. Once the criminal gains access to a bank customer's username and password, the criminal may be able to electronically transfer the bank customer's money to an account maintained by the criminal and abscond with the funds. Electronic transfers are virtually instantaneous. Once the money is released from the bank customer's account the crime is almost always complete. The odds of recovering the funds once they are transferred are negligible.

When a fraudulent electronic transfer occurs, questions arise regarding liability for the loss. The unsuspecting bank customer immediately blames the bank and demands that the bank replace the funds. From the bank customer's perspective, the electronic transfer was not authorized and thus was improper. The customer feels that the unauthorized wire transfer should be treated just like a forged check and the bank should be liable.

Predictably, the bank's view of its liability differs from the bank customer's view. From the bank's perspective, it did nothing wrong. The criminal in most instances gained access to the bank customer's online banking information through the bank customer's computer system, usually by the use of some form of malware. The bank had a security

C. David Hailey is a partner with Mozley, Finlayson & Loggins LLP in Atlanta, Georgia. The author gratefully acknowledges the assistance of Bridgette E. Eckerson, an associate with the firm.

system in place that guarded against fraudulent wire transfers without being unduly burdensome on the bank customer. The bank feels that the customer has an obligation to protect its online bank credentials from computer predators. As noted in a recent decision in this area, the "tension in modern society between security and convenience is on full display" in disputes of this nature.[1]

Liability for fraudulent wire transfers is an important consideration in many fidelity bond claims. The bank may have coverage under its financial institution bond for fraudulent wire transfers from a bank customer's account. However, as will be discussed in this article, the bank may not be liable for the unauthorized activity. Similarly, the bank customer may have coverage for fraudulent wire transfers under its commercial fidelity bond. But if the bank ultimately is liable for the fraud, the bank customer's fidelity carrier may have a subrogation claim against the insured's bank.

The respective obligations and potential liability of the bank and the bank's customer for losses due to fraudulent electronic transfers is the subject of Article 4A of the Uniform Commercial Code.[2] Article 4A aims to provide a uniform set of rules to govern the electronic transfer of funds, rather than an exchange of currency or payment by check.[3]

When a fraudulent funds transfer occurs, the receiving bank often will deny liability.[4] Generally, the bank's denial of liability will be based on the bank's belief that it has a commercially reasonable security procedure in place which, under Article 4A, provides the bank with protection if all the requirements are met.

[1] Choice Escrow & Land Title, LLC v. BancorpSouth Bank, No. 10-03531-CV-S-JTM, 2013 U.S. Dist. LEXIS 36746, at *25 (W.D. Mo. Mar. 18, 2013), *aff'd in part, rev'd in part, and remanded by* 754 F.3d 611 (8th Cir 2014).

[2] U.C.C. § 4A-101 to -507 (2015).

[3] U.C.C. § 4A-102 & official cmt. (2015).

[4] Like all sections of the UCC, Article 4A has its own terminology. The person who initiates the funds transfer, usually a bank customer, is referred to as the "sender." U.C.C. § 4A-103(a)(5) (2015). The wire transfer instructions that the sender gives to its bank are referred to as "payment orders." *Id.* § 4A-103(a)(1). The sender's bank is referred to as the "receiving bank," because it "receives" the payment orders. *Id.* § 4A-103(a)(3).

This article will explore the receiving bank's ability under Article 4A to avoid liability for a fraudulent payment order if it has a "commercially reasonable" security procedure in place. Of necessity, this article will discuss the related issues of whether the particular security measures the bank has in place constitute a "security procedure," and whether the sender and the receiving bank "agreed to" the security procedure. As part of this discussion, this article will consider the impact of the guidance published by Federal Financial Institutions Examination Council ("FFIEC") in 2005 and then supplemented in 2011.[5] This article will also discuss the interplay between the bank's obligation to have a commercially reasonable security system in place and the bank's obligation under Article 4A to act in "good faith."

II.
ANALYSIS UNDER UCC ARTICLE 4A

The receiving bank's potential liability for a fraudulent wire transfer hinges on Sections 201 through 204 of Article 4A. The analysis begins with Section 4A-204, which governs the sender's right to a refund if the receiving bank accepts an unauthorized payment order.[6] In this regard, Section 4A-204(a) provides, in relevant part, as follows:

[5] The FFIEC is comprised of five government agencies involved in the regulation of banks: Board of Governors of Federal Reserve System; Federal Deposit Insurance Corporation; National Credit Union Administration; Office of the Comptroller of the Currency; and Office of Thrift Supervision. On October 12, 2005, the FFIEC issued its initial guidance entitled "Authentication in an Internet Banking Environment." Press Release, Fed. Fin. Insts. Examination Council (Oct. 12, 2005), https://www.ffiec.gov/press/pr101205.htm; FED. FIN. INSTS. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (2005), *available at* https://www.ffiec.gov/pdf/authentication_guidance.pdf [hereinafter 2005 FFIEC GUIDANCE]. On June 28, 2011, the FFIEC issued the "Supplement to Authentication in an Internet Banking Environment." Press Release, Fed. Fin. Inst. Examination Council (June 28, 2011), http://www.ffiec.gov/press/pr062811.htm; FED. FIN. INSTS. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (2011), *available at* https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFEIC%20Formated)pdf [hereinafter 2011 FFIEC SUPPLEMENT].

[6] U.C.C. § 4A-204 (2015).

> If a receiving bank accepts a payment order issued in the name of its customer as sender which is (i) not authorized and not effective as the order of the customer under Section 4A-202, or (ii) not enforceable, in whole or in part, against the customer under Section 4A-203, the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment . . . .[7]

Based on this language, the receiving bank is obligated to refund the money it transferred pursuant to the payment order if the payment order was "not authorized and not effective" under Section 4A-202.[8]

Section 4A-202 contains two subsections. Subsection (a) provides as follows: "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 law of agency."[9] This part of Section 4A-202(a) deals with the "law of agency," as opposed to the more technical concepts associated with security procedures for electronic transfers, and generally is not applicable to payment orders initiated electronically. As noted in the Official Comments to Section 4A-203, the "law of agency" referenced in Section 4A-202(a) may be applicable if the payment order originates by some means other than an online request. In this regard, the Official Comments state as follows:

> In a very large percentage of cases covered by Article 4A, transmission of the payment order is made electronically. The receiving bank may be required to act on the basis of a message that appears on a computer screen. Common law concepts of authority of agent to bind principal are not helpful. There is no way of determining the identity or the authority of the person who caused the message to be sent. The receiving bank is not relying on the authority of any particular person to act for the purported sender. The case is not comparable

[7] *Id.* § 4A-204(a).
[8] *Id.*
[9] U.C.C. § 4A-202(a) (2015).

> to payment of a check by the drawee bank on the basis of a signature that is forged. Rather, the receiving bank relies on a security procedure pursuant to which the authenticity of the message can be "tested" by various devices which are designed to provide certainty that the message is that of the sender identified in the payment order. In the wire transfer business the concept of "authorized" is different from that found in agency law. In that business a payment order is treated as the order of the person in whose name it is issued if it is properly tested pursuant to a security procedure and the order passes the test.[10]

While the prediction in the Official Comments is largely true, the "law of agency" was a determining factor in at least one case involving a payment order generated electronically, and thus it is not safe to assume that general principles of agency law will never apply.[11]

If the receiving bank is unable to establish that Section 4A-202(a) applies, then Section 4A-202(b) provides another exception to the receiving bank's obligation to refund the unauthorized purchase order:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security

[10] U.C.C. § 4A-203 cmt. 1 (2015).

[11] Hedged Inv. Partners, L.P. v. Norwest Bank, Minn., N.A., 578 N.W.2d 765 (Minn. Ct. App. 1998). In the *Hedged* case, a series of unauthorized payment orders were generated electronically by the President of the bank customer. Although the bank failed to follow the agreed-upon security procedure, the bank was able to avoid liability under the law of agency. *See* discussion of *Hedged infra* pp. 103-04. The *Hedged* case differs factually from most cases involving fraudulent payment orders generated electronically in that the person generating the payment orders was affiliated with the bank customer. *See* discussion of *Hedged infra* pp. 103-04.

> against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders in the name of the customer. 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.[12]

As set forth in this language, Section 4A-202(b) requires the receiving bank to meet a number of tests to escape liability for an unauthorized payment order. First, the receiving bank must show that the bank and its customer "agreed that the authenticity of payment orders . . . will be verified pursuant to a security procedure."[13] Then, if the bank is able to show that an "agreed-upon" security procedure was in place, the bank has to show that it complied with both subsections (b)(i) and (b)(ii). Subsection (b)(i) requires the bank to show that the agreed upon security procedure is a "commercially reasonable method of providing security against unauthorized payment orders."[14] Subsection (b)(ii) requires the bank to prove that it accepted the payment order "in good faith and in compliance with the security procedure and any written agreement or instruction of the customer."[15]

Even if the receiving bank is able to establish that the payment order is effective as a payment order of the bank customer under Section 4A-202(b), Article 4A gives the customer an opportunity to shift the liability for a fraudulent payment order back to the receiving bank. Section 4A-203(a)(1) allows the customer to recover if it can show that the receiving bank, by express agreement, limited the extent to which it is entitled to enforce the payment order.[16] Also, the customer can shift liability back to the receiving bank if it can meet the requirements of Section 4A-203(a)(2), which provides as follows:

[12] U.C.C. § 4A-202(b).

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] U.C.C. § 4A-203(a)(1) (2015).

> The receiving bank is not entitled to enforce or retain payment of the payment order if the customer 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.[17]

This exception to the bank's Section 4A-202(b) defense has not given rise to much litigation, perhaps because the majority of cases involving fraudulent wire transfers result from a breach of the bank customer's computer system. The lack of litigation under Section 4A-203(a)(2) also might be due to the acknowledgment of liability by banks if the cybercriminal gained access to the customer's account through the bank's computer system.[18] However, given the importance of this consideration, the bank, bank customer, and fidelity bond insurers should promptly investigate how the cybercriminal gained access to the funds in the bank customer's account.

III.
WHAT IS A SECURITY PROCEDURE?

The first step in deciding whether a security procedure is commercially reasonable is determining whether the security measures the bank has in place to prevent fraud constitute a "security procedure"

[17] *Id.* § 4A-203(a)(2).

[18] At least one case has dealt with this issue, although no resolution of the issue is reported. In *Transamerica Logistic, Inc. v. JPMorgan Chase Bank, N.A.*, No. 4:07-cv-01678, 2008 U.S. Dist. LEXIS 112708, at *7-9 (S.D. Tex. July 21, 2008), the court found that a factual dispute existed as to whether the cybercriminal gained access to the customer's log-in credentials through the customer's computer system or in some other manner.

within the meaning of Article 4A. The beginning point of the analysis is the following definition of "security procedure" in Section 4A-201:

> "Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.[19]

It seems that determining whether a particular procedure is a "security procedure" under Article 4A should be relatively easy, especially because Article 4A contains a definition of "security procedure." However, in some cases the courts have struggled with the concept.

If the security procedure is not overly complex, the analysis is not difficult. For example, in *Insoftvision, LLC v. MB Financial Bank, N.A.*,[20] the bank received a payment order by e-mail. The bank argued that its procedure of acting on the payment order if it was from a recognized e-mail address, without further verification, was a "security procedure" under Article 4A.[21] The court rejected the bank's argument. At best, the court noted, the bank's procedure for acting on an e-mail from a known e-mail address of the sender was "akin to comparing a signature on a written order."[22] Thus, the court held that, "by itself," such a limited procedure cannot be a commercially reasonable "security

[19] U.C.C. § 4A-201 (2015).

[20] No. 10 C 3377, 2011 U.S. Dist. LEXIS 102516 (N.D. Ill. Sept. 12, 2011).

[21] *Id.* at *13-14.

[22] *Id.* at *18.

procedure" based on the last sentence of the definition in Section 4A-201.[23]

As the facts and the security procedures become more complex, the analysis becomes more difficult. In *Hedged Investment Partners, L.P. v. Norwest Bank Minnesota, N.A.*,[24] the court discussed the "security procedure" issue in some detail. The plaintiff in the *Hedged Investment* case was Hedged Investment Partners ("Hedged"), a Minnesota limited partnership, formed to make investments on behalf of third parties.[25] Hedged entered into an "Agency Agreement" with Norwest Bank, pursuant to which the bank agreed to provide wire transfer services to Hedged.[26]

While the Agency Agreement was in place, Hedged initiated twenty-six electronic fund transfers to bank accounts of seven different entities.[27] None of the payment orders were properly authorized pursuant to the procedure set forth in the Agency Agreement.[28] Nineteen of the payment orders were not for legitimate partnership business, although they were initiated and authorized.[29]

One of the many issues discussed in the *Hedged* case was whether the procedures for handling payment orders from Hedged, as set forth in the Agency Agreement, were "security procedures" within the meaning of Article 4A. In its analysis of this issue, the court drew a distinction between "verification" procedures and "authorization" procedures.[30] The court noted that Section 4A-202(a) allowed the bank to escape liability for a fraudulent payment order if the payment order was "authorized" based on the law of agency. On the other hand, according to the court, Section 4A-202(b) deals with "verified" payment orders, and

[23] *Id.*

[24] 578 N.W.2d 765 (Minn. Ct. App. 1998).

[25] *Id.* at 767.

[26] *Id.*

[27] *Id.* at 769.

[28] *Id.*

[29] *Id.*

[30] *Id.* at 773.

requires a "security procedure."[31] The court then analyzed the procedures related to payment orders in the Agency Agreement to determine whether they were designed to "authorize" payment orders under Section 4A-202(a) or to "verify" the authenticity of the payment orders under Section 4A-202(b).[32] If the procedures were designed to "authorize" the payment orders under Section 4A-202(a), then they were not, based on the court's analysis, "security procedures" under Section 4A-202(b).[33]

The Agency Agreement required the bank to (1) retain a copy of the signatures of the limited partners of Hedged to verify communications, and (2) check each new investment advisor's wire transfer instructions by calling the advisor.[34] The court ultimately determined that procedures of this nature were designed to determine whether the payment orders were "authorized" under 4A-202(a), rather than to determine whether the payment orders were "authentic" under 4A-202(b).[35] Based on this analysis, the court held that the procedures were not "security procedures" within the meaning of Article 4A.[36]

[31] *Id.* The court's analysis on this issue was based on the Official Comment to Section 4A-203. The Official Comment does discuss "authorized" payment orders under Section 4A-202(a) and "verified" payment orders under Section 4A-202(b). However, the Official Comment does not make this distinction in the context of determining whether a security measure is a "security procedure" under Section 4A-201.

[32] 578 N.W.2d at 772-74.

[33] *Id.* at 773-74.

[34] *Id.*

[35] *Id.* at 774.

[36] *Id.* Although the analysis in *Hedged* is interesting, it does not appear to have been necessary. This decision under agency law could have been reached without the somewhat confusing analysis of what constitutes a "security procedure." The court remanded the case for a determination of whether the payment orders, which were sent by Hedged's majority owner, president, and consulting general partner, were authorized under the law of agency. On remand, the lower court found that the majority owner was authorized to initiate wire transfers on behalf of Hedged. Thus, the payment orders in question were authorized under the law of agency and the bank was protected by Section 4A-202(a).

In *Chavez v. Mercantil Commercebank, N.A.*,[37] the District Court for the Southern District of Florida utilized an analysis similar to the one in *Hedged*, but reached a somewhat different result. The district court eliminated from consideration as "security procedures" any procedural requirements that were not consistent with the primary purpose of a security procedure under Article 4A. In this regard, the district court based its decision on the language in Section 4A-201 and the Official Comments, holding that a security procedure should be designed to "verify that the identity of the anonymous person on the other side of an electronic transmission is in fact the person who is authorized to make transfers to and from the account."[38] Thus, the court did not consider any procedural requirements that were designed to avoid mistakes, overdrafts, or multiple transfers to be "security procedures" under Article 4A. Instead, a "security procedure" under Article 4A had to be related to the detection of a fraudulent transfer.[39]

Based on this reasoning, the court did not consider checking to make sure that a particular agreement was on file, or checking the account balance to make sure that funds were available, to be part of the bank's security procedure. Similarly, the bank's policy of having two officers review and approve the payment order was not part of the security procedure.[40] However, unlike the court in *Hedged*, the *Chavez* court did consider the identification verification process (requiring identification) and the signature verification process (comparing signatures) to be part of the bank's security procedure.[41] The district court made this distinction, in part, because the payment order was delivered by Chavez "in person," rather than electronically.[42]

[37] No. 10-23244-CIV, 2011 U.S. Dist. LEXIS 126309 (S.D. Fla. Nov. 1, 2011), *rev'd on other grounds*, 701 F.3d 896 (11th Cir. 2012).

[38] *Id.* at *9.

[39] *Id.* at *9-11.

[40] *Id.* at *10-11.

[41] *Id.* at *5-6.

[42] *Id.* at *7-8. The Court of Appeals for the Eleventh Circuit reversed the district court, but not on the issue of whether the bank's security measures were "security procedures." 701 F.3d 896, 903-04 (11th Cir. 2012). The decision was based on the court's analysis of whether the security procedure was an "agreed-upon" security procedure. *See infra* Part IV.

The issue of whether a particular security measure is a "security procedure" can also arise under Section 4A-202(c) if the customer rejects a security procedure offered by the bank. Under Section 4A-202(c), the security procedure the bank actually has in place is deemed to be "commercially reasonable" if the security procedure was chosen by the bank's customer after the bank offered, and the customer refused, another security procedure that was commercially reasonable.[43] In *Experi-Metal, Inc. v. Comerica Bank*,[44] the bank argued, based on Section 4A-202(c), that the customer chose the security procedure in place at the time of the fraudulent payment orders and, in doing so, refused a commercially reasonable security procedure that would have required authorization by more than one person.[45] The court ruled that requiring confirmation of the payment order by additional users was not a security procedure under Article 4A.[46] Thus, the court held that the bank had not offered, and the customer had not refused, a "security procedure" that would have been commercially reasonable.[47]

Filho v. Interaudi Bank[48] demonstrates the importance of taking a consistent position on this issue. At the district court level, the bank argued that all of the procedures described in its "Funds Transfer Policy and Procedures" document were the relevant "security procedures" in the case.[49] One of those procedures required the bank to make a confirming, recorded phone call and for the customer to answer certain security questions during the call.[50] The district court agreed with the bank on this issue.[51]

[43] U.C.C. § 4A-202(c) (2015).

[44] No. 09-14890, 2010 U.S. Dist. LEXIS 68149 (E.D. Mich. July 8, 2010). This is the first of two decisions by the district court in this case.

[45] *Id.* at *13-14.

[46] *Id.* at *14.

[47] *Id.* The court did, however, find that the customer had agreed to another security procedure that was commercially reasonable. *Id.* at *16-17 (secure token technology).

[48] No. 03 Civ. 4795(SAS), 2008 U.S. Dist. LEXIS 31443 (S.D.N.Y. Apr. 16, 2008), *aff'd*, 334 F. App'x 381 (2d Cir. 2009).

[49] 334 F. App'x at 382.

[50] *Id.* at 382 n.1.

[51] 2008 U.S. Dist. LEXIS 31443, at *16-17.

The bank lost the case at trial, presumably because the court determined that it had not followed the phone verification security procedure.[52] On appeal, the bank argued that the trial court erred in finding that the phone verification procedure was a "security procedure" under Article 4A.[53] The Second Circuit summarily rejected the bank's argument.[54]

As these cases illustrate, the question of what security measures are "security procedures" under Article 4A is not as simple as it first appears. Moreover, this issue can have a significant, and sometimes determinative, role in the ultimate outcome of the case. Banks should exercise care in selecting security procedures to ensure that they fall within the definition of Section 4A-201. Bank customers, and their fidelity bond insurers, should carefully analyze the bank's security measures to verify that they are "security procedures" within the meaning of Section 4A-201 before accepting the bank's denial of liability for a fraudulent payment order.

IV.
WAS THE SECURITY PROCEDURE AGREED-UPON?

To avoid liability for a fraudulent payment order, the receiving bank must also show that the bank's customer agreed to the security procedure. This issue also seems to be one that should be relatively easy to resolve. As the case law in the area demonstrates, however, deciding whether the sender and the receiving bank agreed upon a particular security procedure can be difficult.

The decision in *Crabowski v. Bank of Boston*,[55] one of the earliest decisions under Article 4A, illustrates this difficulty. The *Crabowski* case involved a complicated series of bank accounts and related documentation orchestrated by Norman Epstein, the principal of Kinder Capital ("Kinder"), an investment advisory firm. The bank accounts were opened by numerous investors who were clients of

[52] *See* 334 F. App'x at 382 (the Court of Appeals for the Second Circuit's opinion does not state the grounds for the trial court's decision).

[53] *Id.*

[54] *Id.*

[55] 997 F. Supp. 111 (D. Mass. 1997).

Kinder. The stated purpose of the bank accounts was to facilitate the ability of Kinder's customers to invest in "prime bank instruments."[56] Each of the investors executed a "Kinder Power of Attorney," granting Epstein access to the funds in the account, subject to certain limitations, to invest in the "prime bank instruments."[57] These "prime bank instruments" were fictitious, and after the investors deposited their money into the bank accounts in question, Epstein stole the funds through a series of wire transfers from the investors' accounts.[58]

One of the issues in the *Crabowski* case was whether the investors, who were the named owners of the bank accounts in question, had "agreed to" the security procedures that the bank had in place for wire transfers.[59] None of the bank-account-related documentation signed by the investors referenced the bank's security procedures for wire transfers or gave Epstein the power to enter into agreements with the bank on behalf of the customers.[60] However, the bank argued that the power of attorney forms, which were signed by the investors and Epstein, and accepted by the bank, were broad enough to give Epstein the authority to enter into agreements related to security procedures for wire transfers.[61] In support of its argument, the bank described agreements related to security procedures as mere "administrative actions."[62] The bank also argued that because Epstein had agreed to certain security procedures in connection with other bank accounts Kinder had opened in its name, as opposed to the investors' accounts, Epstein had agreed, on behalf of the investors, to the security procedures for the investors' accounts as well.[63]

[56] *Id.* at 115.

[57] *Id.* at 115-18.

[58] *Id.*

[59] *Id.* at 123.

[60] *Id.* at 116. The Kinder Power of Attorney gave Kinder and Epstein the right to give instructions and take all actions on the investors' behalf that were required to operate the account. However, the Kinder Power of Attorney also stated that the account was for the sole purpose of buying and selling the "prime bank instruments."

[61] *Id.* at 123.

[62] *Id.*

[63] *Id.*

The court rejected all of the bank's arguments. In doing so the court noted the basic requirement under Article 4A that the security procedure must be "agreed to" between "the bank and its customer."[64] In its analysis of this issue, the court found that the power of attorney forms executed by the investors did not mention anything about security procedures.[65] The court also determined that the only agreement related to the bank's security procedures was one entered into by Epstein in connection with Kinder's accounts at the bank, not the investors' accounts, and that it was entered into a year before any of the investor accounts were opened.[66]

Skyline International Development v. Citibank,[67] another relatively early decision involving the "agreed-upon" issue, illustrates that the lack of an "agreed-upon" security procedure can work to the benefit of the bank in certain circumstances.[68] In *Skyline*, the bank customer argued that the bank failed to follow the internal security procedures the bank had in place and thus the wire transfer was in violation of Section 4A-202(b).[69] In response, the bank argued that the internal security procedures were not "agreed-to," and thus the customer could not complain that the bank had failed to follow the procedures.[70]

The court held that internal security procedures adopted by the bank, but not known to the customer, were not "agreed-upon" within the meaning of Article 4A.[71] The court in *Skyline* relied upon the definition of "security procedure" in Section 4A-201, which clearly states that a security procedure means "a procedure established by agreement of a customer and a receiving bank."[72] Thus, reasoned the court, the term

[64] *Id.*

[65] *Id.*

[66] *Id.* Given the unusual set of facts, the *Crabowski* court does not appear to stand for the proposition that an agent of a bank customer, with a proper power of attorney, cannot agree to the bank's security procedures on behalf of the customer.

[67] 706 N.E.2d 942 (Ill. App. Ct. 1998).

[68] *Id.* at 945-46.

[69] *Id.* at 945.

[70] *Id.*

[71] *Id.*

[72] *Id.*

"agreed-upon security procedures" does not apply to "procedures the receiving bank may follow unilaterally in processing payment orders."[73]

The "agreed to" issue also can arise, under Section 4A-202(c), in the context of the bank customer's acceptance or rejection of a commercially reasonable security procedure. In *Insoftvision*, the bank argued that it had offered its customer a "commercially reasonable" security procedure, which the customer refused.[74] In support of its argument, the bank noted that when the customer opened its checking account, the bank sent it an information form that asked whether the customer needed any other services, such as wire transfer services.[75] The customer responded by stating "not yet."[76] The bank argued that its request for information was tantamount to an offer of the bank's standard online banking option for wire transfers, which included the bank's standard security procedures.[77] The bank also argued that the customer was familiar with the bank's process for online wire transfers because the administrative employee of the customer involved in online banking had utilized the bank's standard online banking system for wire transfers for another company related to the customer.[78]

The court rejected the bank's arguments. The court noted that the information form merely asked the customer to identify what other services it might need.[79] The form did not mention the bank's online security procedures for such transfers or ask the customer to agree to the security procedures.[80]

While the earlier cases in this area appear to require an express agreement by the customer to the security procedure in question, some of the more recent cases have adopted a more flexible analysis. For

[73] *Id.*

[74] Insoftvision, LLC v. MB Fin. Bank, No. 10 C 3377, 2011 U.S. Dist. LEXIS 102516, at *12 (N.D. Ill. Sept. 12, 2011).

[75] *Id.*

[76] *Id.*

[77] *Id.* at *13.

[78] *Id.*

[79] *Id.*

[80] *Id.* at *12-13.

example, in *Regatos v. North Fork Bank*,[81] the court found that the "agreed-upon" security procedure does not have to be part of an "explicit agreement."[82] In *Regatos*, the bank customer and the bank followed the same procedure for the handling of payment orders over a period of four years.[83] The customer would send the transfer instructions by facsimile and the bank would contact the customer by telephone to confirm the authenticity of the payment order.[84] The bank would then compare the signature on the payment order with the signature it had on file.[85] The customer and the bank followed this procedure for every payment order prior to the fraudulent payment orders at issue in the case.[86] The court held that this consistent course of conduct was sufficient to establish both the existence of a security procedure and that the customer had agreed to the security procedure.[87]

In *Experi-Metal, Inc. v. Comerica Bank*,[88] a more recent case, the court struggled with the "agreed-to" requirement, but ultimately determined that the bank customer had "agreed to" a new security procedure based on language in the related banking agreement.[89] This

[81] 257 F. Supp. 2d 632 (S.D.N.Y. 2003), *aff'd on other grounds*, 431 F.3d 394 (2d Cir. 2005). The main issue on appeal was related to the one-year notice requirement under Section 4A-505. The Court of Appeals for the Second Circuit affirmed the district court's decision on this issue based on the response by the Court of Appeals of New York to certified questions in *Regatos v. North Fork Bank*, 838 N.E.2d 629 (N.Y. 2005).

[82] 257 F. Supp. 2d at 646.

[83] *Id.* at 645.

[84] *Id.* at 646.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] No. 09-14890, 2010 U.S. Dist. LEXIS 68149 (E.D. Mich. July 8, 2010). The underlying dispute in *Experi-Metal* arose out of a "phishing" attack. An employee of Experi-Metal responded to an email that appeared to be from the bank and that contained a link to what appeared to be the bank's website. An Experi-Metal employee "logged into" the fraudulent website, thereby unknowingly giving the cyber-criminal the employee's confidential secure token identification, ID and login information. Over the next six hours, the cybercriminal initiated ninety-three fraudulent payment orders totaling $1,901,269.00. *Id.* at *6-8.

[89] *Id.* at *11-12.

language allowed the bank to change the security procedure upon giving proper notice.[90] When the bank's customer signed the banking agreement, the bank was using "digital certificate technology" as part of its security procedure.[91] The banking agreement identified "digital certificate technology" as the security procedure in place, but further provided that the bank reserved the right to change its security procedures by giving oral or written notice to its customers of any new security measures.[92] The banking agreement further provided that the actual use of any new security procedure, after notice and implementation of the new security procedure, constituted acceptance.[93]

After the banking agreement was signed, the bank implemented "secure token technology."[94] Experi-Metal had used this new technology to conduct routine online banking prior to the fraudulent payment orders, but had not used the new security procedure to initiate any legitimate payment orders. Experi-Metal argued that the secure token technology was not mentioned in the agreement it signed with the bank. Experi-Metal also noted that it had never utilized the new secure token procedure to initiate payment orders. Thus, Experi-Metal reasoned that it had never agreed to the new security procedures for the verification of payment orders.

The court noted, however, that Experi-Metal had used the secure token technology to access its accounts and perform other banking functions.[95] The court also noted that Experi-Metal did not discontinue the use of the service or send the bank a termination notice after the implementation of the new technology, as required by the banking agreement.[96] In this regard, the agreement provided that after receiving written notice of a change, the customer must send a written notice to effectuate termination of the agreement.[97] Thus, the court felt that

[90] *Id.* at *15-16.

[91] *Id.* at *3-6.

[92] *Id.* at *3-5, *11-16.

[93] *Id.*

[94] *Id.* at *5.

[95] *Id.* at *16.

[96] *Id.*

[97] *Id.*

Experi-Metal was aware of the "secure token technology" and had agreed to it.[98]

The court's analysis in *Experi-Metal* is consistent with the decision in *Filho v. Interaudi Bank*.[99] In *Filho*, Filho and his wife (the "Filhos") brought the lawsuit against the bank to recover approximately $950,000 in fraudulent wire transfers from their account at the bank. When the Filhos opened the account, they signed an agreement that governed payment orders sent by any means of communication.[100] The agreement did not describe what security procedures the bank had in place for confirming the authenticity of payment orders. Instead, the agreement authorized the bank to select security procedures that were commercially reasonable.[101] The bank had detailed security procedures in place for authenticating payment orders, but those procedures were outlined in an internal document that was not provided to the Filhos or referenced in the agreement with the Filhos.[102]

The first question the court in *Filho* considered was whether the security procedures, which were never disclosed to the Filhos, were "agreed-upon." The Filhos argued that the bank's ability to unilaterally choose the applicable security procedures did not constitute an agreement.[103] The court conceded that the bank could not establish the "commercial reasonableness" of the security procedure simply by having the customer agree that the procedures are commercially reasonable.[104] However, the court held that a customer could agree that the bank could choose the procedures.[105] The court reasoned that the customer's knowledge as to the specific procedures in place was not required

[98] *Id.* at *17.

[99] No. 03 Civ. 4795(SAS), 2008 U.S. Dist. LEXIS 31443 (S.D.N.Y. Apr. 16, 2008), *aff'd*, 334 F. App'x 381 (2d Cir. 2009). The decision of the Court of Appeals for the Second Circuit was limited to the issue of whether the bank could take an inconsistent position on appeal. *See* discussion *supra* pp. 106-07.

[100] *Id.* at *1.

[101] *Id.* at *1-6.

[102] *Id.* at *3-6.

[103] *Id.* at *14-15.

[104] *Id.* at *16.

[105] *Id.*

because Article 4A required the procedures to be commercially reasonable, regardless of whether they were agreed to or not.[106]

The *Filho* court's logic on the "agreed-upon" issue is questionable. The fact that Article 4A requires the security procedures to be commercially reasonable should not negate the "agreed-upon" requirement even if the customer gives the bank the right to choose the procedures. Nevertheless, the *Filho* case stands for the proposition that a bank can avoid the "agreed-upon" requirement for security procedures by having the customer agree in advance to the procedures the bank chooses, as long as the procedures are commercially reasonable.[107]

The decision in *Filho* should be compared to the decision by the Court of Appeals for the Eleventh Circuit in *Chavez v. Mercantil Commercebank, N.A.*[108] Chavez and the bank entered into an agreement that allowed Chavez to choose one of three security procedures for payment orders delivered "in person."[109] The bank's only obligation under the agreement, based on Chavez's chosen option, was to verify the signature on the payment order.[110] The agreement also permitted the bank, at its option, to use other security procedures to verify the authenticity of payment orders, but the agreement did not describe the procedures or require the bank to utilize the procedures.[111]

The bank's additional security procedures for processing payment orders were set forth in the bank's customer service manual. These additional procedures included checking balance information, verifying that the customer had signed an agreement, and following certain identification procedures.[112] The bank's additional procedures

[106] *Id.*

[107] After the district court decision in *Filho*, which granted partial summary judgment for the bank, the case proceeded to trial and a judgment was entered in favor of Filho based on the bank's failure to follow the "agreed-upon" security procedures. Filho v. Interaudi Bank, 334 F. App'x 381, 382 (2d Cir. 2009).

[108] 701 F.3d 896 (11th Cir. 2012).

[109] *Id.* at 898.

[110] *Id.*

[111] *Id.* at 897-98.

[112] *Id.* at 906.

also required a phone call verification of the payment order, but only if the payment order was delivered by facsimile or mail, rather than "in person." The bank argued that these additional security procedures, implemented by the bank "at its option," were also "agreed to" by the customer, even though the security procedures were not specifically described in the agreement.[113]

The district court had agreed with the bank, holding that these "optional" security procedures were part of the agreed-upon security procedures within the meaning of Article 4A.[114] In so holding, the district court relied upon the *Filho* decision that a bank customer can agree to a security procedure even if the customer is not expressly aware of the procedure.[115]

The Court of Appeals for the Eleventh Circuit reversed the district court's ruling. The decision was based on the Eleventh Circuit's analysis of whether the "additional procedures" the bank could unilaterally select were part of the "agreed-upon security procedure" between Chavez and the bank.[116] The Eleventh Circuit, in construing the agreement in its entirety, did not read the agreement as including the optional identification procedures. The agreement in the *Chavez* case did contain a provision allowing the bank to supplement the specified security procedures to which the customer had agreed.[117] However, the Eleventh Circuit felt that a provision allowing the bank to supplement the security procedures was different from a provision allowing the bank to select the security procedures in the first place.[118] Thus, the Eleventh Circuit distinguished the *Filho* case based on the language in the

[113] *Id.* at 901.

[114] Chavez v. Mercantil Commercebank, N.A., No. 10-23244-CIV, 2011 U.S. Dist. LEXIS 126309 (S.D. Fla. Nov. 1, 2011), *rev'd on other grounds*, 701 F.3d 896 (11th Cir. 2012).

[115] *Id.* at *5-8.

[116] *Chavez*, 701 F.3d at 901-03.

[117] *Id.* at 901.

[118] *Id.* at 901-02.

agreement in *Filho* that allowed the bank to "select security procedures for accepting instructions that are commercially reasonable."[119]

The *Chavez* case and the *Filho* case illustrate the importance of the language in the banking agreement governing payment orders and security procedures. Arguably, if the agreement in the *Chavez* case had given the bank the express authority to select the security procedures, then Chavez would have "agreed" to them, even though Chavez had no specific knowledge of the procedures. In contrast, if the funds transfer agreement provided for a particular security procedure, but allowed the bank to supplement that procedure, the customer may not have "agreed to" any additional procedures within the meaning of Article 4A.

In *Patco Construction Co., Inc. v. People's United Bank*,[120] the "agreed-upon" issue was considered in some detail.[121] The reported decisions in the *Patco* litigation begin with the lengthy discussion of the facts and issues in the magistrate's recommended decision.[122] The Magistrate Decision was adopted by the district court, only to be reversed by the Court of Appeals for the First Circuit.[123]

The *Patco* litigation involved a series of wire transfers generated electronically. While the facts were in dispute on the issue, it appears the cybercriminals were able to capture Patco's login credentials and answers to challenge questions through keystroke malware.[124] After capturing this information, the cybercriminals were able to initiate a series of fraudulent payment orders.[125]

[119] *Id.* (citing Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 U.S. Dist. LEXIS 31443, at *4 (S.D.N.Y. Apr. 16, 2008)).

[120] 684 F.3d 197 (1st Cir. 2012).

[121] *Id.* at 200-01, 208-09.

[122] Patco Constr. Co., Inc. v. People's United Bank, No. 2:09-cv-503-DBH, 2011 U.S. Dist. LEXIS 58112 (D. Me. May 27, 2011) [hereinafter Magistrate Decision].

[123] No. 09-503-P-H, 2011 U.S. Dist. LEXIS 86169 (D. Me. Aug. 4, 2011), *aff'd in part, rev'd in part, and remanded by* 684 F.3d 197 (1st Cir. 2012).

[124] 684 F.3d at 206, 211-13.

[125] *Id.* at 203-06.

The Magistrate Decision discusses the question of whether the security procedures in place at the time were "agreed-upon," and concludes that they were.[126] The decision was easy with respect to the initial written agreements because they were clearly reviewed and signed by Patco representatives. However, these initial agreements provided that the bank could modify them at any time, effective upon publication.[127] The bank claimed that it published some modifications to the initial security procedures on its website before the fraudulent wire transfers were initiated.[128]

With respect to the modifications that were published on the bank's website, the magistrate found that Patco had agreed to those modifications by virtue of the language in the original agreements allowing the bank to modify the terms at any time upon publication.[129] However, not all of the security measures in use by the bank were specifically mentioned in either the original agreement or the published modifications. The published modification language was largely related to the customer's duties to monitor its account and report suspicious activity.[130]

In considering this issue, the Magistrate Decision first noted that Patco had expressly agreed to certain aspects of the bank's security procedures, specifically the use of customer IDs and passwords.[131] The Magistrate Decision also concluded that Patco had agreed "by course of performance" to the use of challenge questions.[132] With respect to other aspects of the bank's security system, which were not mentioned in the original agreement or the modifications, the Magistrate Decision stated that:

> [w]hile other aspects of the Premium Product security system, such as device authentication, IP GEO location, transaction monitoring, and the risk-profiling engine,

[126] 2011 U.S. Dist. LEXIS 58112, at *103-08.
[127] *Id.* at *17.
[128] *Id.* at *14-15.
[129] *Id.* at *106.
[130] *Id.*
[131] *Id.* at *103-04.
[132] *Id.* at *104-05.

> were invisible to Patco, they were integrated with, and largely operated in the service of, the visible portions of the system. Thus, Patco fairly can be said to have agreed to the use of the Premium Product security system *in toto*.[133]

In essence, the Magistrate Decision found that the invisible security measures, which worked together with the visible measures, were agreed to, even though the invisible measures were not mentioned in the initial banking agreement or the online modifications to the initial agreement.[134]

The most recent appellate case in this area is the Eighth Circuit's decision in *Choice Escrow & Land Title, LLC v. BancorpSouth Bank.*[135] In the *Choice Escrow* case, the bank utilized, as part of its security procedure, the PassMark system, a device authentication software.[136] When a bank customer signed up for online banking, the PassMark software stored the IP addresses of the customer's employees who were going to be accessing the system, along with specific information unique to the computers being used by the employees. If the PassMark software detected anything unusual, the system would trigger challenge questions. Choice Escrow argued that the bank's PassMark system should not be considered part of the bank's security procedure because it was not expressly mentioned in any of the agreements between Choice Escrow and the bank.

While the bank's PassMark system was not expressly mentioned in any of the banking agreements, the court found "ample evidence" that

[133] *Id.* at *105-06.

[134] *Id.* The Magistrate Decision, which was adopted by the district court, was reversed by the Court of Appeals for the First Circuit. Unfortunately, the First Circuit did not comment on the "agreed-to" aspect of the Magistrate Decision. Instead, the First Circuit focused on the security procedures in place and found they were not, as implemented, commercially reasonable as a matter of law. Having reached that conclusion, the First Circuit did not have to decide to what extent Patco had agreed to the procedures. Thus, unfortunately, we do not know if the First Circuit would have affirmed the Magistrate Decision's analysis on the "invisible," but agreed-to, security procedures.

[135] 754 F.3d 611 (8th Cir. 2014).

[136] *Id.* at 614.

the parties had agreed to its implementation.[137] In so holding the court noted that while Article 4A requires an "agreed-upon" security procedure, it does not require a written contract.[138] The court then noted that Choice Escrow was required to register for the PassMark system when it signed up for online banking and thus was aware of its existence and use.[139] The court also noted that the bank posted a digital manual entitled "PassMark Login Security" on its online banking portal and that one of the written contracts signed by Choice Escrow referenced "User Manual(s) and Help screens" posted on the portal.[140] Thus, the court felt that "PassMark was incorporated at least implicitly into the parties' written contracts."[141]

The cases illustrate the need for both banks and bank customers to exercise diligence in defining the elements of the bank's security procedures in a written agreement. The bank knows what security procedures it has in place and is in the unique position to explain those procedures to its customer and have the customer agree to them. The bank is also in a position to advise the customer of any changes or additions to the security procedures. Bank customers, on the other hand, need to carefully review this aspect of their agreements with the bank and make sure they understand the security procedures the bank has in place and the risks associated with those procedures. Fidelity bond insurers should carefully evaluate this "agreed-upon" issue in determining whether the bank, or the bank's customer, is liable for the fraudulent payment order.

V.
WHAT IS A COMMERCIALLY REASONABLE SECURITY PROCEDURE?

If the bank is able to show that it had a "security procedure" in place that meets the criteria of Article 4A, and is also able to show that the "security procedure" was "agreed-upon," the threshold tests of Section 4A-202 will have been met. The analysis then turns to the

[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.*

question of whether the agreed-upon security procedure is "commercially reasonable."

Section 4A-202(c) is the starting point for an analysis of whether a security procedure is "commercially reasonable." This section of Article 4A provides as follows:

> Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. 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.[142]

While a detailed explanation of this appears helpful in theory, it has not necessarily been true in practice. Given the number of factors involved and the customer-specific nature of the factors, Article 4A invites a case-by-case, customer-by-customer, analysis. A bank could have a security procedure in place that is "commercially reasonable" for one customer, but not for another, because the needs of the individual customers must be taken into account. Even the apparent "safe harbor" afforded by the bank if the security procedure is "chosen" by the customer is not a complete "safe harbor." The bank still must show that the security procedure the customer refused was commercially reasonable.

[142] U.C.C. § 4A-202(c) (2015).

If the payment order is received by some means other than electronic, the analysis is generally less complicated. In a relatively early case, *Centre-Point Merchant Bank Ltd. v. American Express Bank Ltd.*,[143] the court dealt with the "commercially reasonable" issue in the context of a payment order delivered by telex.[144] *Centre-Point* involved transactions between two banks, Centre-Point Merchant Bank, a Nigerian banking institution, and American Express Bank. Centre-Point opened a bank account at American Express to facilitate certain investment opportunities.[145] Thus, Centre-Point, for purposes of Article 4A, was the bank customer or "sender." One of the issues was whether Centre-Point could recover losses associated with two fraudulent payment orders initiated by a Centre-Point employee.[146]

After Centre-Point and American Express established their banking relationship, almost all communications were by telex.[147] For security purposes, they agreed that all instructions sent by telex would be tested by using a "telegraphic test key code."[148] Unfortunately, the court does not provide any detail as to how the telegraphic test key operated. However, the court noted that Centre-Point's expert admitted that in 1993, when the fraudulent wire transfers occurred, all banks in Nigeria used the telegraphic test key code procedure.[149] The court further noted that this was the security procedure American Express used with all of its correspondent banks and the security procedure Centre-Point used with all of the bank accounts it maintained at other correspondent banks.[150] Thus, the court found this security procedure to be commercially reasonable based on the language in the definition referring to "security procedures in general use by customers and receiving banks similarly situated."[151]

[143] No. 95 Civ. 5000, 2000 U.S. Dist. LEXIS 17296 (S.D.N.Y. Nov. 30, 2000).

[144] *Id.* at *3-4.

[145] *Id.* at *1-3.

[146] *Id.*

[147] *Id.* at *2.

[148] *Id.*

[149] *Id.* at *16.

[150] *Id.* at *14-16

[151] *Id.* at *15 (citing N.Y. U.C.C. § 4-A-202(3)).

The *Regatos* court also considered whether the security procedure in place was "commercially reasonable" in the context of a written payment order.[152] In the *Regatos* case, the payment orders were received by facsimile. The court noted that the comparison of the signatures on the payment orders to the customer's signature card was not, by itself, a security procedure based on the definition in Section 4A-201.[153] However, the court felt that the signature comparison, coupled with phone call confirmation by someone who could recognize Regatos's voice, was a commercially reasonable security procedure for payment orders transmitted to the bank by facsimile.[154]

The *Filho* case also involved payment orders received by facsimile.[155] The court found that the security procedure in place was "commercially reasonable," an issue which the court said was "barely contested" by the Filhos.[156] The security procedure for payment orders received by facsimile included a mandatory signature comparison, telephone confirmation and log, security questions, and identification of the last deposit. The court found this security procedure to be commercially reasonable.[157]

The Filhos argued, based on the *Regatos* case, that the telephone confirmation had to be with a specific bank representative who could recognize their voices, a procedure that was not required in the *Filho*

[152] Regatos v. North Fork Bank, 257 F. Supp. 2d 632, 646 (S.D.N.Y. 2003), *aff'd on other grounds*, 431 F.3d 394 (2d Cir. 2005).

[153] *Id.* at 646.

[154] *Id.* The lower court found that a fact question existed with regard to whether the bank had complied with the agreed upon security procedure. *Id.* at 647. The bank claimed it made confirming phone calls to Regatos. Regatos denied receiving the calls. The case proceeded to trial and Regatos prevailed on that issue. Regatos v. North Fork Bank, 396 F.3d 493, 494 (2d Cir. 2005) (noting that Regatos prevailed at trial). The bank did not appeal the trial outcome, choosing instead to appeal the district court's earlier decision on the issue of whether Regatos had notified the bank of the fraudulent payment order in a timely fashion. *Id.* at 495.

[155] Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 U.S. Dist. LEXIS 31443, at *15 (S.D.N.Y. Apr. 16, 2008), *aff'd*, 334 F. App'x 381 (2d Cir. 2009).

[156] *Id.*

[157] *Id.* at *16-17.

case.[158] However, the court felt that the use of security questions and the telephone log offset this shortcoming.[159] The court also rejected the Filhos' argument that the telephone confirmation process should have included a password or code known to the customer. The court found it unlikely that these measures would have prevented the fraud given the cybercriminal's knowledge of the Filhos' banking relationship.[160]

In the *Experi-Metal* case, the court found that the security procedure in place was commercially reasonable, but provided very little analysis of the issue and adopted a very restrictive view of what evidence should be considered.[161] The court simply stated that "[b]ased on the plain and unambiguous terms" of the banking agreements the bank's secure token technology was commercially reasonable.[162] However, the court did not identify the "plain and unambiguous language" that supports this conclusion. In the preceding section of the opinion, the court quotes several portions of the agreement, including the part where the customer agrees that the procedures in place are commercially reasonable, but the court does not specifically identify the part of the agreement that supports its conclusion.[163]

The *Experi-Metal* court also refused to consider the opinion of Experi-Metal's expert on the "commercially reasonable" issue, based on the parol evidence rule.[164] In this regard, the court simply stated that expert opinion would not be allowed to contradict the "plain language" of the agreements.[165] Again, the "plain language" is not identified. Perhaps the court is referring to the language where the customer agrees that the security procedure is commercially reasonable. If so, the decision is contrary to the plain language in Article 4A and other cases that have correctly noted that Article 4A does not allow the bank to escape its

[158] *Id.* at *17.

[159] *Id.*

[160] *Id.*

[161] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2010 U.S. Dist. LEXIS 68149, at *16-17 (E.D. Mich. July 8, 2010). *See* discussion *supra* pp. 106, 111-12.

[162] *Id.*

[163] *Id.*

[164] *Id.* at *17.

[165] *Id.*

obligation to provide a commercially reasonable security procedure simply by having the customer agree, in advance, that whatever procedure the bank chooses to provide is commercially reasonable.[166]

In the *Chavez* case, the district court's decision included a thorough analysis of the "commercially reasonable" issue.[167] The *Chavez* case involved a wire transfer based on a payment order delivered in person by someone impersonating the bank's customer.[168] When the bank account was opened, Chavez and the bank entered into an agreement that allowed Chavez to choose one of three security procedures for payment orders delivered in person. The bank's only obligation, based on Chavez's chosen option, was to verify the signature on the payment order.[169] The bank also utilized additional security measures for processing payment orders, including checking balance information, verifying the existence of an agreement, and using certain identification procedures.[170]

The district court found the bank's security procedure for in-person payment orders to be commercially reasonable. The agreed-upon security procedures, based on the district court's opinion, included signature verification, coupled with requiring the customer to present identification.[171] In so holding, the court followed the factors outlined in 4A-202(3):

> 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;

[166] Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 U.S. Dist. LEXIS 31443, at *14-15 (S.D.N.Y. Apr. 16, 2008), *aff'd*, 334 F. App'x 381 (2d Cir. 2009); U.C.C. § 4A-202(b).

[167] Chavez v. Mercantil Commercebank, N.A., No. 10-23244-CIV, 2011 U.S. Dist. LEXIS 126309, at *8-14 (S.D. Fla. Nov. 1, 2011), *rev'd*, 701 F.3d 896 (11th Cir. 2012).

[168] *Id.* at *2.

[169] *Id.* at *1-2.

[170] *Id.* The court considered all of these procedures to be part of the "agreed-upon" security procedure.

[171] *Id.* at *11-12.

> alternative security procedures offered to the customer; and security procedures in general use by customers and receiving banks similarly situated.[172]

In assessing these factors, the court relied upon the "unrebutted opinion" of the bank's expert as to the prevailing security standards for "in person" transactions.[173] The court was also influenced by the fact that Chavez did not agree to utilize two alternative security measures that would have provided additional safeguards.[174]

The Eleventh Circuit reversed the district court's ruling.[175] The decision was based on the Eleventh Circuit's analysis of the banking agreement, specifically whether the "additional procedures" the bank could unilaterally choose to use were part of the "agreed-upon" security procedure between Chavez and the bank.[176] Based on the Eleventh Circuit's analysis, the only "agreed-upon" security procedure was signature verification. The Eleventh Circuit held that signature verification was not, by itself, a security procedure.[177]

The analysis of the "commercially reasonable" issue becomes more technical, and more complicated, when the payment orders are initiated electronically. The *Patco* decision, which involves payment orders generated electronically, contains one of the most comprehensive discussions of "commercial reasonableness" under Article 4A.[178]

[172] *Id.* at *8.

[173] *Id.* at *13.

[174] *Id.* at *13-14.

[175] Chavez v. Mercantil Commercebank, N.A., 701 F.3d 896, 901-03 (11th Cir. 2012).

[176] *Id.*

[177] *Id.* at 903-04. *See* discussion *supra* pp 115-16.

[178] Patco Constr. Co., Inc. v. People's United Bank, No. 2:09-cv-503-DBH, 2011 U.S. Dist. LEXIS 58112 (D. Me. May 27, 2011), *adopted*, No. 09-503-P-H, 2011 U.S. Dist. LEXIS 86169 (D. Me. Aug. 4, 2011), *aff'd in part, rev'd in part, and remanded by* 684 F.3d 197 (1st Cir. 2012). The reported decisions in the *Patco* litigation begin with the lengthy discussion of the facts and issues in the Magistrate Decision. The Magistrate Decision was adopted by the district court, only to be reversed by the First Circuit.

While the facts were in dispute on the issue, it appears that the cybercriminals were able to access Patco's bank account through information gathered by keystroke malware.[179] In essence, the cybercriminals were able to capture Patco's login credentials and answers to challenge questions.[180] After capturing this information, the cybercriminals were able to initiate a series of fraudulent payment orders.[181]

The bank in *Patco* utilized the Jack Henry Premium Product ("Premium Product").[182] The Premium Product included a customer ID and password and a user specific ID and password.[183] The system also included challenge questions that were prompted based on a risk profile that considered a multitude of data, including IP location and transaction activity.[184] The Premium Product was also designed to take into account the "circumstances of the customer known to the bank, including size, type, and frequency of payment orders normally issued by the customer to the bank."[185] In this regard, the system had a transaction dollar amount limit above which challenge questions were generated.[186] The system also included a subscription to the eFraud Network, which compared the IP address of the user to IP addresses that were known to have been used for fraudulent activity.[187] The magistrate found this security procedure to be commercially reasonable.[188]

The Magistrate Decision on this aspect of the case might have been correct if all the security measures were utilized as designed. However, one of the security measures was not utilized as designed, which led to a reversal by the First Circuit.[189]

[179] *Patco*, 684 F.3d at 205-06.
[180] *Id.* at 198.
[181] *Id.* at 204-06.
[182] *Patco*, 2011 U.S. Dist. LEXIS 58112, at *33.
[183] *Patco*, 684 F.3d at 202.
[184] *Id.* at 202-03.
[185] *Patco*, 2011 U.S. Dist. LEXIS 58112, at *35.
[186] *Id.* at *37.
[187] *Id.* at *37-38.
[188] *Id.* at *27-34.
[189] *Patco*, 684 F.3d at 197.

The security system in question in *Patco* included a "challenge question" feature if the transaction exceeded a threshold amount.[190] Initially, the bank set the threshold amount at $100,000. However, the bank decided, presumably in an effort to make the system more secure, to lower the threshold amount to $1.00.[191] This decision resulted in the generation of challenge questions for every transaction.[192] Given the prevalence of keystroke malware, which captures the answers to challenge questions, the First Circuit reasoned that the increased use of challenge questions actually increased the cybercriminal's ability to capture the answers to challenge questions.[193] Thus, the First Circuit concluded that this alteration rendered other security measures, which also were designed to trigger challenge questions on high risk transactions, virtually useless.[194]

The First Circuit's decision is interesting because it stands for the proposition that the "commercially reasonable" analysis should go beyond a cursory review of the security procedure in place and actually look at how the security procedure operates. If the bank, for whatever reason, alters a security procedure, even if the bank believes doing so will make the system more secure, the bank runs the risk of compromising the system and removing some of the safeguards. In addition, if the security procedure, without any alterations, is not providing adequate security for the customer because the risk factor settings are not appropriate, the security procedure may not be commercially reasonable. For example, if the customer's usual transaction amount is less than $100,000, but the bank's security procedure only flags transactions above $1 million, the security procedure may not be commercially reasonable for that customer.

The most recent appellate decision in this area is *Choice Escrow & Land Title, LLC v. BancorpSouth Bank.*[195] The *Choice Escrow* case, which involved a payment order generated electronically,[196] is a good

[190] *Id.* at 202.

[191] *Id.* at 203.

[192] *Id.*

[193] *Id.* at 211-12.

[194] *Id.* at 213.

[195] 754 F.3d 611 (8th Cir. 2014).

[196] *Id.* at 613.

illustration of the interplay between the bank and the bank's customer on the issue of what security procedures should be utilized. The bank wants to use the most effective procedure to prevent fraud, but does not want to unduly burden or inconvenience its customer. The bank customer wants to send wire transfers in an efficient manner without involving too many procedures or getting too many people involved in the process. The *Choice Escrow* case also illustrates the potential impact on the bank's customer if it rejects a security procedure recommended by the bank because the procedure is inconvenient.

When Choice Escrow opened its account, the bank typically required its customers to use "dual control," which was a system that necessarily involved two employees.[197] One employee of Choice Escrow had to initiate the payment order, thereby creating a "pending" transaction. Another employee then had to log into the system and release the pending payment order. Choice Escrow declined to use the "dual control" system. In order to utilize the online wire transfer service of the bank without "dual control," Choice Escrow had to sign an agreement acknowledging that it had declined to use "dual control" and that it understood the additional risks it was assuming as a result.

Several months after opening the account, an officer of Choice Escrow received a bulletin warning the company of a recent scam that involved a cybercriminal embedding a "Trojan horse," or keystroke malware, on a victim's computer.[198] The malware allowed the criminal to capture the victim's online banking credentials and initiate fraudulent wire transfers, usually to banks in foreign countries. In response to this bulletin, Choice Escrow asked the bank if it could block wire transfers to foreign banks. The bank responded by stating that it could not place a limitation of that nature on the account and, once again, recommended "dual control." In response, Choice Escrow advised the bank that dual control would not be convenient.

Without "dual control" in place, the bank's security system consisted of the standard customer ID and password, along with device authentication software called PassMark.[199] When a bank customer

[197] *Id.* at 614.

[198] *Id.* at 615.

[199] *Id.* at 614. *See* discussion of PassMark *supra* pp. 118-19.

signed up for online banking, the PassMark software stored the IP addresses of the employees that were going to be accessing the system, along with certain specific information related to the computer being used by the employee.[200] If these security features detected anything unusual, the system would trigger challenge questions.[201]

The cybercriminal in *Choice Escrow* was able to gain access to Choice Escrow's computer system through a phishing attack similar to the attack described in the bulletin Choice Escrow received.[202] The attack resulted in embedded keystroke malware, which allowed the cybercriminal to capture an employee's ID and password, and to mimic the employee's IP address and the characteristics of the employee's computer. Once the cybercriminal had this information the bank's security system was not effective.

Relying on the definition of Section 4A-202(c), and the explanatory language in the Official Comments to Section 4A-203, the court found that the security procedure the bank had in place, along with the "dual control" procedure that Choice Escrow rejected, was commercially reasonable. In so holding the court rejected Choice Escrow's argument that the security system had to include a "transactional analysis," which would involve a manual review of every payment order by a bank employee and should, according to Choice Escrow, differentiate between transactions based on the "size, type, and frequency" of a customer's payment orders.[203]

Although the court rejected the "transactional analysis," the court stated that Article 4A does require the security procedure in place to screen payment orders based on the size, type, and frequency normally issued to the bank by the customer.[204] However, the court further noted that what is commercially reasonable in each case is flexible.[205] Thus, the court refused to "graft a rigid, foreign standard onto the commercial

[200] *Id.*
[201] *Id.* at 613-14.
[202] *Id.* at 615-16.
[203] *Id.* at 618-19.
[204] *Id.* at 619.
[205] *Id.*

reasonableness inquiry," noting that it would be "at odds with essentially all of Article 4A."[206]

Having rejected the "transactional analysis," and having adopted a "flexible" approach, the court shifted to the "broadest level of generality" by looking at "security procedures in general use by customers and receiving banks similarly situated."[207] The court's primary authority was the 2005 FFIEC Guidance.[208] The court felt that the bank's security procedure, which included dual control, was consistent with the 2005 FFIEC Guidance and with the increasing level of sophistication of cybercriminals in the 2009-2010 period.[209]

Despite the detailed analysis of "commercial reasonableness" in *Choice Escrow*, it is clear that the decision was heavily influenced by Choice Escrow's refusal to utilize "dual control" as a matter of convenience. In this regard, the Eighth Circuit summarized its holding on the "commercial reasonableness" issue as follows:

> In short, no genuine dispute of fact exists as to whether BancorpSouth's security procedures were commercially reasonable. Rather, this appears to be a case where "an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper[,]" in which case "the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank." See *Miss. Code Ann.* §75-4A-203 cmt 4. Choice knew that dual control provided a reliable safeguard against Internet fraud, and it explicitly assumed the risks of a lesser procedure notwithstanding the relative ease with which it could have implemented dual control. Accordingly, we conclude that BancorpSouth's security procedures, which included password protection, daily

[206] *Id.*

[207] *Id.*

[208] 2005 FFIEC GUIDANCE, *supra* note 5.

[209] *Choice Escrow*, 754 F.3d at 619-20.

> transfer limits, device authentication, and dual control, were commercially reasonable.[210]

It seems unlikely that the court would have reached the same decision if the bank had not offered, and the customer had not rejected, "dual control."

VI. ROLE OF FFIEC GUIDELINES

In several cases the courts have referred to the 2005 FFIEC Guidance as part of the analysis of the "commercially reasonable" issue.[211] It is obvious that the 2005 FFIEC Guidance has become more significant in recent cases. It also appears that the 2005 FFIEC Guidance will become more important as the fraudulent activity becomes more sophisticated and the security procedures become more complex.

On October 12, 2005, the FFIEC agencies issued an initial "guidance" entitled "Authentication In An Internet Banking

[210] *Id.* at 622.

[211] 2005 FFIEC GUIDANCE, *supra* note 5. The 2005 FFIEC Guidance was referred to specifically in *Patco Construction Co., Inc. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012), and *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611 (8th Cir. 2014). In *All American Siding & Windows, Inc. v. Bank of America, National Association*, 367 S.W.3d 490 (Tex. Ct. App. 2012), a recent appellate court decision in Texas, one of the issues considered by the court was whether the agreed upon security procedures were commercially reasonable under 4A-202. The bank's security procedures consisted of a customer ID and password, and a digital certificate specific to the customer's browser. *Id.* at 494. Without any meaningful analysis, the court concluded that the security procedures were commercially reasonable. *Id.* at 500-02. The court referenced the 2005 FFIEC Guidance in its opinion, but did not provide any analysis of how the security procedure was consistent with the recommendations in the 2005 FFIEC Guidance. *Id.* at 500-01.

Environment."[212] The FFIEC agencies later summarized the 2005 FFIEC Guidance as follows:

> The 2005 Guidance provided a risk management framework for financial institutions offering Internet-based products and services to their customers. It stated that institutions should use effective methods to authenticate the identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information. The Guidance provided minimum supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds to other parties. The 2005 Guidance also provided that institutions should perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing internal and external threats.[213]

The 2005 FFIEC Guidance lists various methods of authentication, or "factors." In this regard, the 2005 FFIEC Guidance notes that existing authentication methodologies involve three basic "factors":

> *Something a person knows*–commonly a password or PIN. If the user types in the correct password or PIN, access is granted.
>
> *Something a person has*–most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.

[212] 2005 FFIEC GUIDANCE, *supra* note 5.

[213] 2011 FFIEC SUPPLEMENT, *supra* note 5, at 1.

> *Something a person is*–most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.[214]

The 2005 FFIEC Guidance also states as follows:

> The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and electronic commerce activities, including account inquiry, bill payment, and account aggregation. However, financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming, malware, and the evolving sophistication of compromised techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.[215]

Clearly, the 2005 FFIEC Guidance requires "multifactor" authentication for transactions involving the "movement of funds to other parties," such as online wire transfers. An appropriate multi-factor authentication security procedure would require at least two of the three factors noted in the guidelines: *something a person knows, something a person has, and something a person is.*

In the "Appendix," the 2005 FFIEC Guidance provides a more detailed list of authentication techniques, processes, and methodologies that a bank can use as part of its security procedure. This section of the

[214] 2005 FFIEC GUIDANCE, *supra* note 5, app. at 7.

[215] *Id.* at 4 (internal footnotes omitted).

2005 FFIEC Guidance lists the following specific security techniques: Shared Secrets, Tokens, Biometrics, Non-Hardware-Based One-Time-Password Scratch Card, Out-of-Band Authentication, Internet Protocol Address (IPA) Location and Geo Location, Mutual Authentication, and Customer Verification Techniques.[216]

In 2011, the FFIEC agencies issued the "Supplement to Authentication in an Internet Environment."[217] The stated purpose of the 2011 FFIEC Supplement is as follows:

> The purpose of this Supplement to the 2005 Guidance (Supplement) is to reinforce the Guidance's risk management framework and update the Agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment. The Supplement reiterates and reinforces the expectations described in the 2005 Guidance that financial institutions should perform periodic risk assessments considering new and evolving threats to online accounts and adjust their customer authentication, layered security, and other controls as appropriate in response to identified risks. It establishes minimum control expectations for certain online banking activities and identifies controls that are less effective in the current environment. It also identifies certain specific minimum elements that should be part of an institution's customer awareness and education program.[218]

This stated purpose for the 2011 FFIEC Supplement is reinforced in the "Background" section, which notes the increased level of criminal activity related to electronic transfers and the increased sophistication of the cybercriminals involved.[219]

In order to combat the increased risk, the 2011 FFIEC Supplement stresses the expectation that financial institutions will

[216] *Id*. app. at 8-14.

[217] 2011 FFIEC SUPPLEMENT, *supra* note 5.

[218] *Id.* at 1.

[219] *Id.* at 2.

perform periodic risk assessments and adjust their customer authentication controls appropriately in response to their findings.[220] The 2011 FFIEC Supplement states that financial institutions should implement layered security, utilizing controls consistent with the increased level of risk for business transactions.[221] The 2011 FFIEC Supplement further recommends multifactor authentication for business customers.[222]

The 2011 FFIEC Supplement goes on to describe the meaning of "layered security" and lists effective controls that may be included in a layered security program. "Layered security," according to the 2011 FFIEC Supplement, "is characterized by the use of different controls at different points in the transaction process so that a weakness in one control is generally compensated for by the strength of a different control."[223] A number of effective controls are listed in the 2011 FFIEC Supplement, including such measures as fraud detection systems based on a customer's typical behavior, dual control, out-of-band verification, transactional limits, IP recognition, limitations on customer control over administrative functions, and enhanced customer education.[224]

The 2011 FFIEC Supplement also discussed the lack of effectiveness of certain authentication techniques relied upon in the past by financial institutions. In this regard, the 2011 FFIEC Supplement notes that simple device identification and challenge questions are easily manipulated by cybercriminals.[225]

As illustrated by this discussion of the 2005 FFIEC Guidance and the 2011 FFIEC Supplement, this is a highly technical area and it remains to be seen to what extent the courts will adopt these publications as the standard for determining whether a given security procedure is "commercially reasonable" under Article 4A. Nothing in the 2005 FFIEC Guidance or the 2011 FFIEC Supplement suggests that they were prepared for that purpose. However, the courts in *Patco* and *Choice*

[220] *Id.* at 3.
[221] *Id.* at 4-5.
[222] *Id.* at 4.
[223] *Id.*
[224] *Id.* at 4-5.
[225] *Id.* at 6-7.

Escrow did look to the 2005 FFIEC Guidance in connection with their analyses of the security procedure the banks had in place.

VII.
GOOD FAITH

If the bank is able to show that it had a security procedure in place, and is further able to show that the customer "agreed to" the security procedure, then the bank can try to show that it should not be liable for a fraudulent payment order because the security procedure was commercially reasonable. However, the analysis of the bank's liability does not end there. Under Section 4A-202(b), the bank must also show that it acted in "good faith" in connection with the transaction.[226]

The term "good faith" in the context of wire transfers means "honesty in fact and the observance of reasonable commercial standards of fair dealing."[227] The "honesty in fact" prong is subjective. The "observance of reasonable commercial standards of fair dealing" prong is objective.[228]

In the *Chavez* case, the district court seems to have focused on the subjective part of the definition of good faith, finding that the bank acted in good faith in accepting the payment orders for processing.[229] In so holding, the court noted that the absence of "good faith" requires something more than negligence. Rather than negligence, the district court felt that the conduct of the bank must be dishonest or reckless.[230] As an example, the court used the failure of the bank to inquire if the identification documentation had obvious irregularities.[231] The district court also seems to have placed the burden of proof on the bank

[226] U.C.C. § 4A-202(b)(ii) (2015).

[227] U.C.C. § 4A-105(a)(6) (2015).

[228] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2011 U.S. Dist. LEXIS 62677, at *30-31 (E.D. Mich. June 13, 2011). This is the second district court opinion involving the *Experi-Metal* case.

[229] Chavez v. Mercantil Commercebank, N.A., No. 10-23244-CIV, 2011 Dist. LEXIS 126309, at *14-17 (S.D. Fla. Nov. 1, 2011), *rev'd on other grounds*, 701 F.3d 896 (11th Cir. 2012).

[230] *Id.* at *16.

[231] *Id.*

customer to show the absence of "good faith." In this regard, the court noted Chavez's failure to offer any evidence that the bank should have suspected that the identification was false.[232]

The Court of Appeals for the Eleventh Circuit reversed the lower court's ruling.[233] The decision was based on the Eleventh Circuit's analysis of the banking agreement, specifically whether the "additional procedures" that the bank could unilaterally choose to use were part of the "agreed-upon security procedure" between Chavez and the bank.[234] Thus, unfortunately, the Eleventh Circuit did not address the district court's decision on the good faith issue.[235]

In the first *Experi-Metal* decision, the district court granted the bank's motion for summary judgment on the "commercially reasonable" issue.[236] However, the district court did not grant the bank's motion for summary judgment on the "good faith" requirement, finding instead that questions of fact existed as to the bank's "good faith" in accepting the payment orders for processing.[237]

After a bench trial, the district court in *Experi-Metal*, in its second opinion, ruled that the bank failed to establish that it had acted in good faith.[238] In so ruling, the court noted that the modern definition of "good faith" under the UCC contains both a subjective, honesty-in-fact requirement, and an objective, "fair dealings" requirement.[239] The court noted that the complete definition of the "fair dealings" requirement under the UCC is the "observance of reasonable commercial standards of fair dealing."[240] The evidence did not support any finding of dishonest

[232] *Id.* at *16-17.

[233] *Chavez*, 701 F.3d at 901-03.

[234] *Id.*

[235] *Id.*

[236] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2010 U.S. Dist. LEXIS 68149, at *16-18 (E.D. Mich. July 8, 2010).

[237] *Id.* at *18-21.

[238] Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2011 U.S. Dist. LEXIS 62677, at *38 (E.D. Mich. June 13, 2011).

[239] *Id.* at *28-30.

[240] *Id.* at *29.

conduct by the bank, so the court focused on the "fair dealings" requirement.[241]

The court noted several facts indicative of the bank's lack of good faith, including the testimony of Experi-Metal's expert.[242] In this regard, Experi-Metal argued that the bank failed to implement fraud scoring or fraud screening, which would have detected the unusual nature of the fraudulent transactions, as compared to Experi-Metal's normal wire transfer activity. Prior to the fraudulent payment orders, Experi-Metal had initiated only two wire transfers. In contrast, the cybercriminal initiated ninety-three payment orders in a six-hour period. Experi-Metal also noted that the fraudulent payment orders requested transfers to foreign destinations (Moscow, Estonia, and China), which was inconsistent with Experi-Metal's normal wire transfer activity. Experi-Metal's expert also suggested that most banks had implemented some form of monitoring systems to detect fraud. Experi-Metal also argued that the 2005 FFIEC Guidance required banks to have the "express security mechanisms outlined in the [guidelines]."

The district court in *Experi-Metal* did not seem particularly impressed with these arguments. The district court did not find that a fraud monitoring system was required for the bank to have acted in "good faith."[243] The court further noted that Experi-Metal's expert was not specific as to how many banks or which banks had implemented fraud monitoring.[244] The court also rejected Experi-Metal's arguments based on the 2005 FFIEC Guidance.[245]

While the court was skeptical of Experi-Metal's evidence on the "good faith" issue, the court was even less impressed with the bank's evidence. The court noted that the bank had focused almost exclusively on the subjective intent of its employees, rather than the bank's "observance of reasonable commercial standards for fair dealing."[246] The court found that the "good faith" standard requires more than the old

[241] *Id.* at *29-30.
[242] *Id.* at *31-33.
[243] *Id.* at *33-35.
[244] *Id.* at *33.
[245] *Id.* at *32-34.
[246] *Id.* at *30, *33-35.

"pure heart and empty head" standard and thus no longer hinges on the bank's "motives."[247] According to the court, the bank failed to present evidence from which the court could conclude what "reasonable commercial standards of fair dealing" were for the bank in responding to a phishing incident such as the one in question.[248] Without any evidence of the "fair dealing" standards, the bank was unable to present evidence that it had complied with the standard.[249] The court also noted that the bank's expert had no experience with internet banking systems and thus was not qualified to testify on the issue.[250]

The decision in *Experi-Metal* on the good faith issue ultimately turned on the burden of proof. The court concluded that the bank had the burden of showing that it acted in "good faith."[251] After considering all the evidence, the court held that the bank failed to carry its burden.[252]

In the *Choice Escrow* case, the bank customer argued that the bank failed to act in "good faith" in connection with the fraudulent wire transfer.[253] In addressing this issue, the court noted the apparent overlap between the requirement of a "commercially reasonable security procedure" and the banks obligation to act in good faith, which means, in part, the "observance of reasonable commercial standards of fair dealing."[254] The court conceded that there may be some evidentiary overlap, but felt that the two inquiries were "coextensive."[255] In reconciling the two concepts, the court held that "technical compliance with a security procedure is not enough under Article 4A."[256] Instead, "the bank must abide by its procedures in a way that reflects the parties' reasonable expectations as to how those procedures will operate."[257]

[247] *Id.* at *34.

[248] *Id.*

[249] *Id.* at *33-35.

[250] *Id.* at *35-36.

[251] *Id.* at *28-29.

[252] *Id.* at *37-38.

[253] Choice Escrow & Land Title, LLC v. BancorpSouth Bank, 754 F.3d 611, 622 (8th Cir. 2014).

[254] *Id.* at 623.

[255] *Id.*

[256] *Id.*

[257] *Id.*

With regard to Choice Escrow's expectations, the court noted that Choice Escrow was well aware of the automated nature of the process and that the role of the bank's employees was not to check for any irregularities.[258] The court further noted that the wire transfer in question was not so irregular as to have caused suspicion, even if the bank was required to review it manually.[259] The bank submitted evidence that the wire transfer in question was not the largest Choice Escrow had ever initiated and that Choice Escrow's wire transfers did not follow a particular pattern.[260] The court also rejected Choice Escrow's argument that the bank should have noticed that the memo line on the payment order, which read "invoice:equipment," was inconsistent with Choice Escrow's business.[261] In rejecting this argument, the court held that it was not realistic to expect the bank's employees to be familiar with the business of all of its customers or to ensure that the memo line in the payment order is consistent with that business purpose.[262] The court distinguished the *Experi-Metal* case on the basis that it involved overdrafts totaling $5 million from a single account that usually had no balance.[263]

These cases illustrate the importance of the "good faith" requirement. Even if the bank has a commercially reasonable security procedure in place, the bank must still show that it acted in good faith. Based on the decisions in *Chavez* and *Choice Escrow*, it is clear that the "good faith" analysis is subjective and, at least arguably, more flexible than the "commercially reasonable" standard. The "reasonable expectations" language in the *Choice Escrow* case would seem to allow for a variety of arguments by the customer. While the case law on this issue is limited, the most important consideration appears to be whether the fraudulent transactions are markedly different from the bank customer's normal wire transfer activity. In *Experi-Metal*, the court was influenced by the large number of fraudulent transactions over a short period of time, which was a distinctive departure from the customer's normal wire transfer activity. In contrast, the *Choice Escrow* court noted

[258] *Id.* at 619.

[259] *Id.* at 623-24.

[260] *Id.* at 624.

[261] *Id.*

[262] *Id.*

[263] *Id.*

that the wire transfer was not so irregular as to have caused suspicion. However, other irregularities, such as the ultimate destination of the funds or the recipient of the funds, should be considered in the analysis as well.

These cases also illustrate that banks should take the "good faith" requirement seriously, and not just rely on the old "honesty in fact" definition or assume that the customer must show the absence of "good faith." If the bank ignores the need for evidence of its good faith, and ignores its burden of proof, the bank may find itself in the same position as the bank in *Choice Escrow*, a case where the bank lost the "good faith" argument despite the lack of persuasive evidence on the issue from the bank customer.

VIII.
CONCLUSION

Determining whether the bank had a commercially reasonable security procedure in place is a multi-part analysis that is often difficult. The analysis is critically important, however, in determining whether the receiving bank or the bank's customer is liable for a fraudulent payment order. The analysis involves an initial determination of whether the particular security measures that the bank has in place constitute a "security procedure" as defined in Article 4A. While this analysis would appear to be relatively simple, it can be complicated, and is often a determining factor in whether the security procedure is "commercially reasonable."

Next, the security procedure must be "agreed-upon" between the receiving bank and the sender. This issue can be as difficult as determining whether two parties have agreed to any other contractual provision. The analysis may be even more difficult because of the tendency of banks to modify security procedures unilaterally, often utilizing on-line notification procedures. Many of the security procedures are highly technical in nature, and thus difficult to communicate. However, banks could do a much better job of communicating the technical aspects of their security procedures and explaining any optional security procedures to their customers.

Ultimately, the court must decide whether the "agreed-upon" security procedure in place is "commercially reasonable." Based on the language in Article 4A, this is a case-by-case analysis based on a variety of factors. What is "commercially reasonable" for one bank may not be "commercially reasonable" for another bank. Moreover, what is required for one customer may not be the same for another customer of the same bank. Banks are required to assess the needs of its customers in this area and design security procedures to fit those needs. While it is not clear at this time, it appears that the FFIEC Guidance will play an increased role in this analysis as security procedures become more complex and cybercriminals become more adept at circumventing the procedures.

Even if the bank has a "commercially reasonable" security procedure in place, the bank still must act in "good faith." This analysis, which is both subjective and objective, requires that the bank show the "observance of reasonable commercial standards of fair dealing." As the case law in this area demonstrates, it may be more difficult to prove "good faith" than it is to show that the security procedure in place was "commercially reasonable." The analysis of the two issues overlaps to a certain extent, but the "good faith" analysis tends to focus more on the characteristics of the bank customer's typical wire transfer activity and the bank customer's reasonable expectations.

Of course, the ultimate decision on liability has ramification for fidelity bond carriers. If the bank is responsible, the loss might be covered by the bank's financial institution bond. Similarly, if the bank customer is responsible, the loss might be covered by the customer's fidelity bond. In order to properly analyze a fidelity claim in this area, practitioners should become familiar with the requirements of Article 4A and how the courts have interpreted and applied those requirements.