APPEAL NO. 13-1879
CROSS APEAL NO. 13-1931

In the
UNITED STATES COURT OF APPEALS
for the
EIGHTH CIRCUIT

Choice Escrow and Land Title, LLC,
Plaintiff – Appellant/Cross-Appellee,

v.

BancorpSouth Bank,
Defendant – Appellee/Cross-Appellant.

On Appeal from the United States District Court for the Western District of Missouri,
Case No. 6:10-CV-03531-JTM,
The Honorable John T. Maughmer, Magistrate Judge.

APPELLANT'S ADDENDUM

Jeff McCurry
Bruce McCurry

CHANEY & McCURRY
3249 E. Ridgeview Street
Springfield, MO 65804
417-887-4141 (Phone)
417-887-4177 (Fax)

Leland L. Gannaway

GANNAWAY & CUMMINGS
3249 E. Ridgeview Street
Springfield, MO 65804
417-887-4141 (Phone)
417-887-4177 (Fax)

Attorneys for Plaintiff – Appellant/Cross-Appellee
Choice Escrow and Land Title, LLC

APPELLANT'S ADDENDUM

IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHERN DIVISION

Choice Escrow and Land Title, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 10-03531-CV-S-JTM**
	)	
BancorpSouth Bank,	)	
	)	
Defendant.	)	

ORDER

In 2010, plaintiff Choice Escrow and Land Title, LLC ("Choice") maintained a trust account with defendant BancorpSouth Bank ("BSB"). On March 17, 2010, BSB received an internet-based request to make a wire transfer of $440,000.00 out of Choice's trust account through BSB's internet wire transfer system. BSB thereafter transferred $440,000 to an intermediary bank [Bank of New York] which then transferred the funds to an institution in the Republic of Cypress, as a beneficiary for an entity identified only as "Brolaw Services, Ltd."

The present litigation ensued with Choice suing BSB, arguing that it "ha[d] never heard of, done business with, or held money in escrow for Brolaw," that it did not initiate, approve, authorize, or ratify the March 17, 2009 wire transfer, and that the wire transfer was fraudulently initiated by an unknown third party. Choice's claims arise under the "Funds Transfers Act" provisions of the Uniform Commercial Code ("UCC") as adopted by Mississippi, MISS. CODE ANN. §§ 75-4A-101, *et seq* (Rev. 2002). Presently pending before the Court is PLAINTIFF'S FIRST MOTION FOR SUMMARY JUDGMENT [Doc. 159], PLAINTIFF'S SECOND MOTION FOR SUMMARY JUDGMENT [Doc. 163], and the MOTION OF DEFENDANT BANCORPSOUTH BANK FOR SUMMARY JUDGMENT [Doc. 160]. The Court will take up the latter motion first.

At the heart of BSB's summary judgment motion – and at the center of the entire litigation – is the question of who should bear the risk of loss when a wire transfer is fraudulently undertaken by a third-party unconnected to either the issuing bank or its customer. With regard to the allocation of such risk, the Funds Transfers provisions of the Uniform Commercial Code ("UCC"), enacted in the State of Mississippi at MISS. CODE ANN. §§ 75-4A-101, *et seq.*,[1] provide guidance. Initially, as a general rule, unless otherwise provided in the UCC, the risk of loss for unauthorized transfers lies with a bank. MISS. CODE ANN. § 75-4A-204.

In its summary judgment motion, BSB asserts that the exception to the general rule as codified in the UCC applies and relieves it of liability. To that end, the law provides:

> 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 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 issued 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.

MISS. CODE. ANN. § 75-4A-202(b) (*emphasis added*). Thus, the risk of loss for an unauthorized transaction will lie with a customer if the bank can establish that its "security procedure is a commercially reasonable method of providing security against unauthorized payment orders," and "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 issued in the name of the customer."

---

[1] The parties are in seeming agreement that Mississippi UCC law applies, though Missouri UCC law appears to be identical. *See* MO. REV. STAT. §§ 400.4A-101, *et seq.*

However, notwithstanding the foregoing, a customer still will not have to bear the risk of loss over an unauthorized transaction if the customer can prove that the unauthorized transaction order "was not caused, directly or indirectly," by any person:

> (1) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or
>
> (2) 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[2] facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault.

MISS. CODE. ANN. § 75-4A-203(a)(2)(i)-(ii).

As noted above, in its motion for summary judgment, BSB argues that – as a matter of law – the risk of loss associated with the unauthorized $440,000 wire transfer on March 17, 2009, lies with Choice. In order for BSB to prevail, the Court must be satisfied that there are no genuine issues of material fact regarding:

> (1) whether BSB's security procedure was a commercially reasonable method of providing security against unauthorized payment orders,
>
> (2) whether BSB accepted the $440,000 payment order in good faith and in compliance with the security procedure and any written agreement or instruction of Choice restricting acceptance of payment orders issued in the name of the Choice, and
>
> (3) whether the fraudster(s) who initiated the unauthorized transfer obtained the necessary security information from a source controlled by Choice and without authority of BSB.[3]

BSB has the burden of proving the first two points. MISS. CODE. ANN. § 75-4A-202(b) The burden on the third point, however, shifts to Choice. MISS. CODE. ANN. § 75-4A-203(a)(2)

---

[2] The statute defines "information" to encompass "any access device, computer software, or the like." Miss. Code. Ann. § 75-4A-203(a)(2).

[3] There is no contention that the subject $440,000 wire transfer was an "inside job" undertaken with the knowledge and cooperation of employees of Choice.

I. BSB's security procedure is deemed a commercially reasonable method of providing security against unauthorized payment orders.

The Funds Transfers provisions of the UCC contain a basic definition of a "security procedure," noting that the term includes any "procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication." MISS. CODE ANN. § 75-4A-201. The statute further notes that a security procedure "may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices." MISS. CODE ANN. § 75-4A-201. The Funds Transfers provisions of the UCC also contain guidance regarding a determination of "commercial reasonableness," to wit:

> 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.

MISS. CODE ANN. § 75-4A-202(c).

In this case, BSB argues that its security procedure must be "deemed to be commercially reasonable" under the second sentence of Section 202(c). Consequently, BSB must establish that:

(1) a security procedure was chosen by Choice after BSB offered, and Choice refused, a security procedure that was commercially reasonable for Choice, and

(2) Choice expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BSB in compliance with the security procedure that was selected by Choice.

As set out herein, based on the summary judgment record before the Court, BSB establishes both of these requirements.

On April 16, 2009, Choice established an account with BSB to be utilized as an escrow/trust account. Shortly after opening this account, Choice determined that it wished to utilize a BSB online banking product ("InView") so as to have the ability to wire transfer funds electronically. In essence, the InView system allowed a BSB customer to effectuate a wire transfer of funds via the Internet by utilizing a User ID and password assigned to the customer by BSB.

In 2009, BSB typically required its customers enrolling in the InView system to utilize "Dual Control," which meant that an electronic wire transfer could only be effectuated by two individuals using separate User IDs and passwords. Basically, one individual would enter and approve the requested wire transfer in the InView system; however, no funds would be released until a second individual logged on to the InView system and released the funds. Choice declined the use of "Dual Control." Consistent with its policy,[4] BSB had Choice execute a MEMO on May 6, 2009, that stated (with emphasis in the original):

> We, Choice Escrow and Land Title, LLC, and all related entities which utilize [BSB's] InView Wire Module to transact online wire requests, understand the additional risks we assume by waiving

[4] If a customer refused to utilize "Dual Control," BSB would permit the customer to make electronic wire transfer of funds through the InView system if the customer would sign an agreement acknowledging it was waiving the use of "Dual Control" and the additional risks associated with such a waiver.

> [BSB's] requirement to utilize Dual Control for outgoing wires. By signing below we understand that although InView can restrict the account from which wires are sent and the amount related to said wire, InView **CANNOT** restrict to where the wire is sent.
>
> Since we wish to waive Dual Control anyone who has a User ID and Password or obtains access to a user ID and Password can wire funds to any other financial institution without restriction by [BSB] or the InView system. We understand that this can occur if our password is stolen. Further if funds are fraudulently wired out in this manner there is a substantial probability that we will be unable to retrieve our funds or recover losses.

The same day that Choice signed the above-quoted Dual Control waiver, it completed paperwork with BSB designating two of its employees (Cara Thulin and Brooke Black) as authorized to "enter," "approve," "release," and "cancel" wire transfers from Choice's escrow account at BSB. To that end, the designation form also provided:

> If desired, enter a daily wire transfer limit to apply at the company level. When this daily limit is reached, users at the company may not approve or release additional wire transfers on that day. (Note: Regardless of company or user limits for higher amounts, an account's current ledger balance will govern whether or not a wire transfer can be processed.)

In designating Ms. Thulin and Ms. Black, Choice declined to place a daily transfer limit on either employee, and Choice further declined to put a daily limit on the daily transfers for Choice company-wide.

In November of 2009, a Choice employee (Jim Payne) received an e-mail from one of its underwriters containing an "Escrow Bulletin" that warned of a scam whereby a fraudster would embed a "Trojan horse" on to a victim's computer, collect the victim's passwords, and then (using the passwords) wire funds from the victim's account to foreign banks. On November 11, 2009, Mr. Payne forwarded the e-mail to BSB and asked whether wire transfers to foreign banks could be limited. Two days later, Ashley Kester with BSB responded:

> Hi Jim, sorry to just now be responding. I had to do some research to find out if this was possible. We are unable to stop just foreign wires, the solution is Dual Control. We always recommend Dual Control on wires. We discussed this when we set up InView and you decided to waive Dual Control. Would you like to consider adding it now? This is the best solution, that way if someone in the company is compromised then the hacker would not be able to initiate a wire with just one user's information. Let me know, thanks!

Mr. Payne responded to this e-mail within a few minutes by asking for the "mechanics" of Dual Control and noting that it "[s]ound[ed] as if it would be a good precaution." Ms. Kester thereafter e-mailed Mr. Payne and informed him:

> It will take two people within InView to send a wire. One person to enter and another to approve/send. We will need to alter our agreements and will send the changes to you.

However, a half-hour later, Mr. Payne responded to Ms. Kester's e-mail:

> Actually, I don't think that would be a good procedure for us – lots of time Paige [Payne, a Choice employee] is here by herself and that would be really tough unless we all shared passwords.

Ms. Kester acknowledged Mr. Payne's e-mail, noting everything would be left as it was and informing Mr. Payne to let her know "if [Choice] would like to make any changes." Between the e-mail exchange on November 13, 2009, and March 17, 2010, no changes were made to Choice's InView procedures.

Between May 6, 2009 (when the InView access was created for Choice), and March 17, 2010, Ms. Thulin and Ms. Black made over 250 wire transfers on behalf of Choice using the InView system to send funds to numerous individuals, companies and financial institutions, including some wire transfers exceeding $400,000. The transfers made by Ms. Thulin and Ms. Black did not follow any routine schedule or pattern regarding the amount, the recipient, or destination. In addition, approximately 87% of the wire transfer requests made by Choice

through the InView system left blank the "Originator Bank Information" field – essentially a field permitting Choice to add a "memo line" to its request (akin to a memo line on a paper check).

Near noon on March 17, 2010, BSB received a wire transfer request via the InView system requesting a transfer of funds in the amount of $440,000 from Choice's escrow account for the benefit of Brolaw Services, Ltd. ("the Brolaw request"). The Brolaw request noted that the receiver bank was the Bank of New York, but that the beneficiary's bank (*i.e.*, the ultimate destination of the funds) was the Popular Bank Public Co. Ltd., an institution in the Republic of Cyprus. The Brolaw request was initiated using the InView User ID and password assigned to Ms. Black and was initiated from the IP address registered to Choice (and confirmed by BSB when Choice's access to InView was created). In addition, upon receipt of the Brolaw request, BSB authenticated that Ms. Black's computer was being used to make the request by detecting the secure device ID token that BSB had previously downloaded to Ms. Black's computer.

At 12:54 p.m., a BSB employee (Brenda Dulaney) confirmed that all of the information necessary to process the Brolaw request had been inputted. Ms. Dulaney then released the request for further processing within BSB's system. In particular, this processing included:

(1) checking the parties and accounts identified in the Brolaw request against the "black list" of terrorist individuals and organizations maintained by the Office of Foreign Assets Control, and

(2) checking the balance of funds available in Choice's escrow account to confirm the sufficiency of the funds.

The Brolaw request cleared this further processing – no terrorist connections were triggered and Choice had sufficient funds in its escrow account.

After Ms. Dulaney released the funds, BSB automatically generated a Transaction Receipt that was faxed to Choice and received by Choice at 12:54:30 p.m. on March 17.

Sometime thereafter, the Transaction Receipt was moved from Choice's fax machine to a shipping table where it was found by Choice employee (Paige Payne) the next morning. After determining that no Choice employee had requested the transfer, Choice contacted BSB and notified it that the Brolaw request was unauthorized. BSB then undertook efforts through the FBI, the State Department and the U.S. Embassy in Cyprus to recover the funds, but it was unsuccessful.

As previously noted, a security procedure must be "deemed to be commercially reasonable" under the second sentence of Section 202(c) in this case if:

> (1) a security procedure was chosen by Choice after BSB offered, and Choice refused, a security procedure that was commercially reasonable for Choice, and
>
> (2) Choice expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BSB in compliance with the security procedure that was selected by Choice.

Based on the summary judgment record, the Court finds that both of these criteria have been established within the requirements of FED. R. CIV. P. 56.

As detailed above, on two different occasions, Choice was offered the opportunity to employ "Dual Control" as part of its utilization of BSB's InView system and Choice refused the option on both occasions. There can be little doubt that "Dual Control" meets the definition of a security procedure as set out in MISS. CODE ANN. § 75-4A-201. Thus the first element comes down to whether "Dual Control" was commercially reasonable for Choice.

Choice argues that "Dual Control" was not commercially reasonable for it because "at times, one or both of the two individuals authorized to perform wire transfers through the InView system [Ms. Black and Ms. Thulin] were out of the office due to various reasons." The Court disagrees. As set out in the UCC as adopted by Mississippi, the determination of what is

commercially reasonable is a question of law – which the Court believes imposes an objective test of reasonableness. Viewing the summary judgment record, the Court finds that the opportunity to use "Dual Control" was commercially reasonable. The record discloses that Ms. Black and Ms. Thulin were both in the office most days. Even assuming that Choice did not want to designate a third employee as an emergency back-up, the likelihood that both Ms. Black and Ms. Thulin would be unavailable for extended periods was small and represented more of an inconvenience to Choice rather than an impediment. As noted in the Official Comments to the Funds Transfers provisions of the UCC:

> The purpose of [having a security procedure deemed to be commercially reasonable] is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available. . . . Sometimes 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 that case, under the last sentence of subsection (c), the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank.

U.C.C. § 4A-203 (Official Comment) (*emphasis added*). The Official Comment further notes the obvious: "a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable." *Id.*

However, the Court finds that the "Dual Control" option offered by BSB and refused by Choice did meet the prevailing standards for good banking practices. This is borne out in the testimony of BSB's expert witness as well as Choice's expert (Brad Maryman). As to the latter, Mr. Maryman gave the following testimony:

Q: Would you also agree that dual control as we've just been discussing it with all of these assumptions[5] . . . would be a commercially reasonable security procedure?

A: I believe it could, yes.

Having determined that BSB's "Dual Control" security procedure was offered to Choice, was refused by Choice, and was commercially reasonable for Choice, the Court briefly addresses the final requirement, namely that Choice must have expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BSB in compliance with the security procedure that was selected by Choice. The Court finds that this requirement has been satisfied. In addition to the agreements previously quoted, Choice executed a Funds Transfer Agreement. Among other matters, this agreement provides that "[a]ny request received by [BSB] with the valid security code shall be irrebutably presumed to be from [Choice's authorized employees]. The Funds Transfer Agreement also explicitly states:

> [Choice] hereby authorizes [BSB] to honor, execute, and charge to [Choice's] account(s) any and all requests or orders to transfer or to pay funds through InView. [BSB] is authorized to complete all such transactions on [Choice's] account(s), which are initiated through the use of [Choice's] access code. [Choice] assumes full responsibility and risk of loss for all transactions made by [BSB] in good faith reliance upon [Client's] request or orders through InView. . . .

The Court finds BSB's security procedure was a commercially reasonable method of providing security against unauthorized payment orders under MISS. CODE. ANN. § 75-4A-202(b)(i).

II. BSB accepted the Brolaw request in good faith and in compliance with the security procedure and any written agreement or instructions of Choice restricting acceptance of payment orders issued in the name of Choice.

---

[5] Mr. Maryman was asked to assume that Ms. Black and Ms. Thulin had separate computers and did not share User IDs and passwords.

Inasmuch as the Court finds that BSB's security procedure was a commercially reasonable method of providing security against unauthorized payment orders, the Court must next turn to the second requirement of the UCC's risk-shifting statute wherein BSB must 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 restricting acceptance of payment orders issued in the name of the customer.

MISS. CODE. ANN. § 75-4A-202(b)(ii)

The definition for good faith is set forth in the UCC and encompasses "honesty in fact and the observance of reasonable commercial standards of fair dealing." MISS. CODE. ANN. § 75-4A-105(6). Consequently, there is both an objective and subjective component to good faith. With regard to objective good faith, there is little case law on the subject *vis-à-vis* the Funds Transfers provisions of the UCC, but the Court generally agrees with the test formulated by the Maine Supreme Court:

> The factfinder must . . . determine, first, whether the conduct of the holder comported with industry or "commercial" standards applicable to the transaction and, second, whether those standards were reasonable standards intended to result in fair dealing. Each of those determinations must be made in the context of the transaction at hand.

Maine Family Credit Union v. Sun Life Assurance Co. of Canada, 727 A.2d 335, 343 (Me. 1999). *See also Experi-Metal, Inc. v. Comerica Bank*, 2011 WL 2433383, op. at *12 (E.D. Mich. Jun. 13, 2011) (applying the *Maine Family Credit Union* standard to the Funds Transfers provisions of the UCC).

Applying that test, the Court finds that that the record is sufficient to establish that there are no genuine disputes with regard to the material facts as to whether BSB comported with industry or "commercial" standards and whether those standards were reasonable standards intended to result in fair dealing. The parties and their respective experts are in agreement that

the Federal Financial Institutions Examination Council's 2005 Guidance ("FFEIC 2005 Guidance") provides the applicable standards. The Court finds that BSB provided unrefuted evidence that it comported with industry standard as set forth in the FFEIC 2005 Guidelines, in particular as they relate to the use of multi-factor identification in providing for security procedures.[6] Finally, although it is surely self-evident, the Court finds the standards included in the FFEIC 2005 Guidelines with regard to security procedures were reasonable standards intended to result in fair dealing.

In its summary judgment pleadings, Choice makes no argument that BSB did not act honestly in accepting the Brolaw request on March 17, 2010. Nonetheless, the Court has reviewed the summary judgment record and is satisfied that BSB has established for purposes of Fed. R. Civ. 56 that it acted in subjective good faith in processing the Brolaw request.

Finally, as previously addressed, the Court finds that the payment of the Brolaw request by BSB was in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The Court would simply add that it does find any written agreements between BSB and Choice

---

[6] Essentially, Choice argues that BSB's security procedure was a single-factor authentication and thus contrary to the FFEIC 2005 Guidelines. The FFEIC 2005 Guidelines describe three different methodologies for authenticating customers:

(1) something known only to the user (e.g., User IDs and/or passwords);

(2) something only the user has (e.g., an ATM card, a specific IP address, a computer security token); and

(3) something the user fundamentally is (e.g., a biometric characteristic such as a fingerprint or voice recognition).

The FFEIC 2005 Guidelines required the use of two or more of these factors to constitute an acceptable multi-factor authentication. The Court finds that Choice's argument that BSB's security was a single-factor authentication to not be supported by evidence and, indeed, contrary to the record before the Court.

to be defective or ineffectual merely because BSB's internal Passmark system (which authenticated the Choice computer through the detection of a secure device ID token) was not mentioned in any of the agreements. In addition, the Court does not find that Mr. Payne's e-mail in November of 2009 asking whether BSB could limit transfers to foreign banks was an instruction by Choice restricting BSB's ability to accept payment orders.

Consequently, based on the foregoing, the Court finds that BSB has met its burden of proving consistent with Fed. R. Civ. P. 56 that the requirements of MISS. CODE. ANN. § 75-4A-202(b) have been met. As a result, pursuant to the intent of the drafters of the UCC, the risk of loss for the unauthorized wire transfer on March 17, 2010, shifts to Choice.

One final matter must be addressed. As the Court noted previously, even if the risk-shifting conditions of Section 202(b) are met, a customer may still prevail if it can satisfy the requirements of Section 203(a)(2). Under that statute, a customer still will not have to bear the risk of loss over an unauthorized transaction if the customer can prove that the unauthorized transaction order "was not caused, directly or indirectly," by any person:

> (1) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or
>
> (2) 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.

MISS. CODE. ANN. § 75-4A-203(a)(2)(i)-(ii).

Choice makes no argument for relief under Section 203(a)(2). Accordingly, the Court will simply note that, although there is no evidence that Choice employees were involved in the fraud, it does appear from the summary judgment record that the fraudster(s) effectively hacked into Ms. Black's computer to accomplish the March 17, 2010 transfer. There is no evidence that

the fraudster(s) was/were acting under the authority or permission of BSB. Consequently, Section 203(a)(2) provides no relief to Choice from the risk-shifting application of Section 202(b).

The tension in modern society between security and convenience is on full display in this litigation. Choice understandably feels as though it did nothing wrong, but yet is out $440,000. BSB, as well, feels as though it has done nothing wrong. In essence, both parties are correct – yet someone must bear the risk of loss. While such a risk generally would lie with a banking institution, the UCC has delineated a particular circumstance where the risk should be shifted to the customer. This case falls within that exception.

The result is not wholly unjust. The experts in this case agree that the fraud would not likely have occurred if Choice had utilized the "Dual Control." It elected not to . . . twice. In refusing the option the first time, Choice agreed that:

> Since we wish to waive Dual Control anyone who has a User ID and Password or obtains access to a user ID and Password can wire funds to any other financial institution without restriction by [BSB] or the InView system. We understand that this can occur if our password is stolen. Further if funds are fraudulently wired out in this manner there is a substantial probability that we will be unable to retrieve our funds or recover losses.

Unfortunately, that is exactly what came to pass. In refusing the "Dual Control" option the second time, Choice ignored BSB's admonition:

> We always recommend Dual Control on wires. We discussed this when we set up InView and you decided to waive Dual Control. Would you like to consider adding it now? <u>This is the best solution, that way if someone in the company is compromised then the hacker would not be able to initiate a wire with just one user's information</u>.

Again, unfortunately, this appears to be exactly what happened.

For the foregoing reasons, the Court **GRANTS** the MOTION OF DEFENDANT BANCORPSOUTH FOR SUMMARY JUDGMENT [Doc. 160]. All other pending motions, including all other motions for summary judgment (including motions for partial summary judgment), are **DENIED** as moot. Accordingly, it is

ORDERED that summary judgment is entered in favor or defendant BancorpSouth Bank.

/s/ John T. Maughmer
John T. Maughmer
United States Magistrate Judge

West's Annotated Mississippi Code
Title 75. Regulation of Trade, Commerce and Investments
Chapter 4A. Uniform Commercial Code--Funds Transfers
Part 1. Subject Matter and Definitions

Miss. Code Ann. § 75-4A-102

§ 75-4A-102. Subject Matter

Currentness

Except as otherwise provided in Section 75-4A-108, this chapter applies to funds transfers defined in Section 75-4A-104.

Credits
Laws 1991, Ch. 316, § 1, eff. July 1, 1991.

Editors' Notes

UNIFORM COMMERCIAL CODE COMMENT

Article 4A governs a specialized method of payment referred to in the Article as a funds transfer but also commonly referred to in the commercial community as a wholesale wire transfer. A funds transfer is made by means of one or more payment orders. The scope of Article 4A is determined by the definitions of "payment order" and "funds transfer" found in Section 4A-103 and Section 4A-104.

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

In the drafting of Article 4A, a deliberate decision was made to write on a clean slate and to treat a funds transfer as a unique method of payment to be governed by unique rules that address the particular issues raised by this method of payment. A deliberate decision was also made to use precise and detailed rules to assign responsibility, define behavioral norms, allocate risks and establish limits on liability, rather than to rely on broadly stated, flexible principles. In the drafting of these rules, a critical consideration was that the various parties to funds transfers need to be able to predict risk with certainty, to insure against risk, to adjust operational and security procedures, and to price funds transfer services appropriately. This consideration is particularly important given the very large amounts of money that are involved in funds transfers.

Funds transfers involve competing interests--those of the banks that provide funds transfer services and the commercial and financial organizations that use the services, as well as the public interest. These competing interests were represented in the drafting process and they were thoroughly considered. The rules that emerged represent a careful and delicate balancing of those interests and are intended to be the exclusive means of determining the rights, duties and liabilities of the affected parties in any situation covered by particular provisions of the Article. Consequently, resort to principles of law or equity outside of Article 4A is not appropriate to create rights, duties and liabilities inconsistent with those stated in this Article.

West's Annotated Mississippi Code
Title 75. Regulation of Trade, Commerce and Investments
Chapter 4A. Uniform Commercial Code--Funds Transfers
Part 2. Issue and Acceptance of Payment Order

Miss. Code Ann. § 75-4A-201

§ 75-4A-201. Security Procedure

Currentness

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

Credits
Laws 1991, Ch. 316, § 1, eff. July 1, 1991.

Editors' Notes

UNIFORM COMMERCIAL CODE COMMENT

A large percentage of payment orders and communications amending or cancelling payment orders are transmitted electronically and it is standard practice to use security procedures that are designed to assure the authenticity of the message. Security procedures can also be used to detect error in the content of messages or to detect payment orders that are transmitted by mistake as in the case of multiple transmission of the same payment order. Security procedures might also apply to communications that are transmitted by telephone or in writing. Section 4A-201 defines these security procedures. The definition of security procedure limits the term to a procedure "established by agreement of a customer and a receiving bank." The term does not apply to procedures that the receiving bank may follow unilaterally in processing payment orders. The question of whether loss that may result from the transmission of a spurious or erroneous payment order will be borne by the receiving bank or the sender or purported sender is affected by whether a security procedure was or was not in effect and whether there was or was not compliance with the procedure. Security procedures are referred to in Sections 4A-202 and 4A-203, which deal with authorized and verified payment orders, and Section 4A-205, which deals with erroneous payment orders.

Miss. Code Ann. § 75-4A-201, MS ST § 75-4A-201
Current through End of 2012 Regular Session

End of Document

West's Annotated Mississippi Code
Title 75. Regulation of Trade, Commerce and Investments
Chapter 4A. Uniform Commercial Code--Funds Transfers
Part 2. Issue and Acceptance of Payment Order

Miss. Code Ann. § 75-4A-202

§ 75-4A-202. Authorized and Verified Payment Orders

Currentness

(a) A payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency.

(b) 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 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 issued 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.

(c) 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.

(d) The term "sender" in this chapter includes the customer in whose name a payment order is issued if the order is the authorized order of the customer under subsection (a), or it is effective as the order of the customer under subsection (b).

(e) This section applies to amendments and cancellations of payment orders to the same extent it applies to payment orders.

(f) Except as provided in this section and in Section 75-4A-203(a)(1), rights and obligations arising under this section or Section 75-4A-203 may not be varied by agreement.

Credits
Laws 1991, Ch. 316, § 1, eff. July 1, 1991.

Editors' Notes

UNIFORM COMMERCIAL CODE COMMENT

This section is discussed in the Comment following Section 4A-203.

Miss. Code Ann. § 75-4A-202, MS ST § 75-4A-202
Current through End of 2012 Regular Session

End of Document

West's Annotated Mississippi Code
Title 75. Regulation of Trade, Commerce and Investments
Chapter 4A. Uniform Commercial Code--Funds Transfers
Part 2. Issue and Acceptance of Payment Order

Miss. Code Ann. § 75-4A-203

§ 75-4A-203. Unenforceability of Certain Verified Payment Orders

Currentness

(a) If an accepted payment order is not, under Section 75-4A-202(a), an authorized order of a customer identified as sender, but is effective as an order of the customer pursuant to Section 75-4A-202(b), the following rules apply:

(1) By express written agreement, the receiving bank may limit the extent to which it is entitled to enforce or retain payment of the payment order.

(2) 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.

(b) This section applies to amendments of payment orders to the same extent it applies to payment orders.

Credits
Laws 1991, Ch. 316, § 1, eff. July 1, 1991.

Editors' Notes

UNIFORM COMMERCIAL CODE COMMENT

1. Some person will always be identified as the sender of a payment order. Acceptance of the order by the receiving bank is based on a belief by the bank that the order was authorized by the person identified as the sender. If the receiving bank is the beneficiary's bank acceptance means that the receiving bank is obliged to pay the beneficiary. If the receiving bank is not the beneficiary's bank, acceptance means that the receiving bank has executed the sender's order and is obliged to pay the bank that accepted the order issued in execution of the sender's order. In either case the receiving bank may suffer a loss unless it is entitled to enforce payment of the payment order that it accepted. If the person identified as the sender of the order refuses to pay on the ground that the order was not authorized by that person, what are the rights of the receiving bank? In the absence of a statute or agreement that specifically addresses the issue, the question usually will be resolved by the law of agency. In some cases, the law of agency works well. For example, suppose the receiving bank executes a payment order given by means of a letter apparently written by a corporation that is a customer of the bank and apparently signed by an officer of the corporation. If the receiving bank acts solely on the basis of the letter, the corporation is not bound as the sender of the payment order unless the signature was that of the officer and the officer was authorized to act for the corporation in the issuance of payment orders, or some other

agency doctrine such as apparent authority or estoppel causes the corporation to be bound. Estoppel can be illustrated by the following example. Suppose P is aware that A, who is unauthorized to act for P, has fraudulently misrepresented to T that A is authorized to act for P. T believes A and is about to rely on the misrepresentation. If P does not notify T of the true facts although P could easily do so, P may be estopped from denying A's lack of authority. A similar result could follow if the failure to notify T is the result of negligence rather than a deliberate decision. Restatement, Second, Agency § 8B. Other equitable principles such as subrogation or restitution might also allow a receiving bank to recover with respect to an unauthorized payment order that it accepted. In Gatoil (U.S.A.), Inc. v. Forest Hill State Bank, 1 U.C.C. Rep.Serv.2d 171 (D.Md.1986), a joint venturer not authorized to order payments from the account of the joint venture, ordered a funds transfer from the account. The transfer paid a bona fide debt of the joint venture. Although the transfer was unauthorized the court refused to require recredit of the account because the joint venture suffered no loss. The result can be rationalized on the basis of subrogation of the receiving bank to the right of the beneficiary of the funds transfer to receive the payment from the joint venture.

But in most cases these legal principles give the receiving bank very little protection in the case of an authorized payment order. Cases like those just discussed are not typical of the way that most payment orders are transmitted and accepted, and such cases are likely to become even less common. Given the large amount of the typical payment order, a prudent receiving bank will be unwilling to accept a payment order unless it has assurance that the order is what it purports to be. This assurance is normally provided by security procedures described in Section 4A-201.

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 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.

Section 4A-202 reflects the reality of the wire transfer business. A person in whose name a payment order is issued is considered to be the sender of the order if the order is "authorized" as stated in subsection (a) or if the order is "verified" pursuant to a security procedure in compliance with subsection (b). If subsection (b) does not apply, the question of whether the customer is responsible for the order is determined by the law of agency. The issue is one of actual or apparent authority of the person who caused the order to be issued in the name of the customer. In some cases the law of agency might allow the customer to be bound by an unauthorized order if conduct of the customer can be used to find an estoppel against the customer to deny that the order was unauthorized. If the customer is bound by the order under any of these agency doctrines, subsection (a) treats the order as authorized and thus the customer is deemed to be the sender of the order. In most cases, however, subsection (b) will apply. In that event there is no need to make an agency law analysis to determine authority. Under Section 4A-202, the issue of liability of the purported sender of the payment order will be determined by agency law only if the receiving bank did not comply with subsection (b).

2. The scope of Section 4A-202 can be illustrated by the following cases. *Case #1.* A payment order purporting to be that of Customer is received by Receiving Bank but the order was fraudulently transmitted by a person who had no authority to act for Customer. *Case #2.* An authentic payment order was sent by Customer, but before the order was received by Receiving Bank the order was fraudulently altered by an unauthorized person to change the beneficiary. *Case #3.* An authentic payment order was received by Receiving Bank, but before the order was executed by Receiving Bank a person who had no authority to act for Customer fraudulently sent a communication purporting to amend the order by changing the beneficiary. In each case Receiving Bank acted on the fraudulent communication by accepting the payment order. These cases are all essentially similar and they are treated identically by Section 4A-202. In each case Receiving Bank acted on a communication that it thought was

authorized by Customer when in fact the communication was fraudulent. No distinction is made between Case #1 in which Customer took no part at all in the transaction and Case #2 and Case #3 in which an authentic order was fraudulently altered or amended by an unauthorized person. If subsection (b) does not apply, each case is governed by subsection (a). If there are no additional facts on which an estoppel might be found, Customer is not responsible in Case #1 for the fraudulently issued payment order, in Case #2 for the fraudulent alteration or in Case #3 for the fraudulent amendment. Thus, in each case Customer is not liable to pay the order and Receiving Bank takes the loss. The only remedy of Receiving Bank is to seek recovery from the person who received payment as beneficiary of the fraudulent order. If there was verification in compliance with subsection (b), Customer will take the loss unless Section 4A-203 applies.

3. Subsection (b) of Section 4A-202 is based on the assumption that losses due to fraudulent payment orders can best be avoided by the use of commercially reasonable security procedures, and that the use of such procedures should be encouraged. The subsection is designed to protect both the customer and the receiving bank. A receiving bank needs to be able to rely on objective criteria to determine whether it can safely act on a payment order. Employees of the bank can be trained to "test" a payment order according to the various steps specified in the security procedure. The bank is responsible for the acts of these employees. Subsection (b)(ii) requires the bank to prove that it accepted the payment order in good faith and "in compliance with the security procedure." If the fraud was not detected because the bank's employee did not perform the acts required by the security procedure, the bank has not complied. Subsection (b)(ii) also requires the bank to prove that it complied with any agreement or instruction that restricts acceptance of payment orders issued in the name of the customer. A customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank. For example, the customer may prohibit the bank from accepting a payment order that is not payable from an authorized account, that exceeds the credit balance in specified accounts of the customer, or that exceeds some other amount. Another limitation may relate to the beneficiary. The customer may provide the bank with a list of authorized beneficiaries and prohibit acceptance of any payment order to a beneficiary not appearing on the list. Such limitations may be incorporated into the security procedure itself or they may be covered by a separate agreement or instruction. In either case, the bank must comply with the limitations if the conditions stated in subsection (b) are met. Normally limitations on acceptance would be incorporated into an agreement between the customer and the receiving bank, but in some cases the instruction might be unilaterally given by the customer. If standing instructions or an agreement state limitations on the ability of the receiving bank to act, provision must be made for later modification of the limitations. Normally this would be done by an agreement that specifies particular procedures to be followed. Thus, subsection (b) states that the receiving bank is not required to follow an instruction that violates a written agreement. The receiving bank is not bound by an instruction unless it has adequate notice of it. Subsections (25), (26) and (27) of Section 1-201 apply.

Subsection (b)(i) assures that the interests of the customer will be protected by providing an incentive to a bank to make available to the customer a security procedure that is commercially reasonable. If a commercially reasonable security procedure is not made available to the customer, subsection (b) does not apply. The result is that subsection (a) applies and the bank acts at its peril in accepting a payment order that may be unauthorized. Prudent banking practice may require that security procedures be utilized in virtually all cases except for those in which personal contact between the customer and the bank eliminates the possibility of an unauthorized order. The burden of making available commercially reasonable security procedures is imposed on receiving banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud. The burden on the customer is to supervise its employees to assure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached.

4. The principal issue that is likely to arise in litigation involving subsection (b) is whether the security procedure in effect when a fraudulent payment order was accepted was commercially reasonable. The concept of what is commercially reasonable in a given case is flexible. Verification entails labor and equipment costs that can vary greatly depending upon the degree of security that is sought. A customer that transmits very large numbers of payment orders in very large amounts may desire and may reasonably expect to be provided with state-of-the-art procedures that provide maximum security. But the expense involved may make use of a state-of-the-art procedure infeasible for a customer that normally transmits payments orders infrequently or in relatively low amounts. Another variable is the type of receiving bank. It is reasonable to require large money center banks

to make available state-of-the-art security procedures. On the other hand, the same requirement may not be reasonable for a small country bank. A receiving bank might have several security procedures that are designed to meet the varying needs of different customers. The type of payment order is another variable. For example, in a wholesale wire transfer, each payment order is normally transmitted electronically and individually. A testing procedure will be individually applied to each payment order. In funds transfers to be made by means of an automated clearing house many payment orders are incorporated into an electronic device such as a magnetic tape that is physically delivered. Testing of the individual payment orders is not feasible. Thus, a different kind of security procedure must be adopted to take into account the different mode of transmission.

The issue of whether a particular security procedure is commercially reasonable is a question of law. Whether the receiving bank complied with the procedure is a question of fact. It is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers. The purpose of subsection (b) is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard. On the other hand, a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable. Subsection (c) states factors to be considered by the judge in making the determination of commercial reasonableness. Sometimes 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 that case, under the last sentence of subsection (c), the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank. But this result follows only if the customer expressly agrees in writing to assume that risk. It is implicit in the last sentence of subsection (c) that a bank that accedes to the wishes of its customer in this regard is not acting in bad faith by so doing so long as the customer is made aware of the risk. In all cases, however, a receiving bank cannot get the benefit of subsection (b) unless it has made available to the customer a security procedure that is commercially reasonable and suitable for use by that customer. In most cases, the mutual interest of bank and customer to protect against fraud should lead to agreement to a security procedure which is commercially reasonable.

5. The effect of Section 4A-202(b) is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure. An exception to this result is provided by Section 4A-203(a)(2). The customer may avoid the loss resulting from such a payment order if the customer can prove that the fraud was not committed by a person described in that subsection. Breach of a commercially reasonable security procedure requires that the person committing the fraud have knowledge of how the procedure works and knowledge of codes, identifying devices, and the like. That person may also need access to transmitting facilities through an access device or other software in order to breach the security procedure. This confidential information must be obtained either from a source controlled by the customer or from a source controlled by the receiving bank. If the customer can prove that the person committing the fraud did not obtain the confidential information from an agent or former agent of the customer or from a source controlled by the customer, the loss is shifted to the bank. "Prove" is defined in Section 4A-105(a)(7). Because of bank regulation requirements, in this kind of case there will always be a criminal investigation as well as an internal investigation of the bank to determine the probable explanation for the breach of security. Because a funds transfer fraud usually will involve a very large amount of money, both the criminal investigation and the internal investigation are likely to be thorough. In some cases there may be an investigation by bank examiners as well. Frequently, these investigations will develop evidence of who is at fault and the cause of the loss. The customer will have access to evidence developed in these investigations and that evidence can be used by the customer in meeting its burden of proof.

6. The effect of Section 4A-202(b) may also be changed by an agreement meeting the requirements of Section 4A-203(a)(1). Some customers may be unwilling to take all or part of the risk of loss with respect to unauthorized payment orders even if all of the requirements of Section 4A-202(b) are met. By virtue of Section 4A-203(a)(1), a receiving bank may assume all of

the risk of loss with respect to unauthorized payment orders or the customer and bank may agree that losses from unauthorized payment orders are to be divided as provided in the agreement.

7. In a large majority of cases the sender of a payment order is a bank. In many cases in which there is a bank sender, both the sender and the receiving bank will be members of a funds transfer system over which the payment order is transmitted. Since Section 4A-202(f) does not prohibit a funds transfer system rule from varying rights and obligations under Section 4A-202, a rule of the funds transfer system can determine how loss due to an unauthorized payment order from a participating bank to another participating bank is to be allocated. A funds transfer system rule, however, cannot change the rights of a customer that is not a participating bank. § 4A-501(b). Section 4A-202(f) also prevents variation by agreement except to the extent stated.

Miss. Code Ann. § 75-4A-203, MS ST § 75-4A-203
Current through End of 2012 Regular Session

End of Document

H

Only the Westlaw citation is currently available.

United States District Court,
E.D. Michigan,
Southern Division.
EXPERI–METAL, INC., Plaintiff,
v.
COMERICA BANK, Defendant.

No. 09–14890.
June 13, 2011.

Richard B. Tomlinson, Troy, MI, for Plaintiff.

Boyd White, III, Lara L. Kapalla, Todd A. Holleman, Detroit, MI, Henry J. Stancato, Troy, MI, for Defendant.

BENCH OPINION

PATRICK J. DUGGAN, District Judge.

*1 This matter arises from a "phishing" [FN1] attack on January 22, 2009, that resulted in a criminal hijacking the bank accounts Plaintiff Experi–Metal, Inc. ("Experi–Metal") maintained with Defendant Comerica Bank ("Comerica" or "bank") and wire transferring more than $1.9 million from those accounts to destinations around the globe. Experi–Metal filed this action against Comerica on November 17, 2009, seeking to hold Comerica liable for the approximately $560,000 in stolen funds that were not recovered. In its Complaint, Experi–Metal alleges that the risk of loss for the unauthorized wire transfers falls upon Comerica pursuant to Michigan Compiled Laws sections 440.4601 –4957.[FN2] This decision follows a bench trial with respect to Experi–Metal's claim, held on January 19–26, 2011.

FN1. "Phishing" has been described as:

> The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.
>
> http://www.webopedia.com/term/p/phishing.html.

FN2. Experi–Metal filed its Complaint in the Circuit Court for Macomb County, Michigan. On December 17, 2009, Comerica removed the Complaint to this Court based on diversity jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1441.

I. Applicable Law and Resolved and Remaining Issues

Comerica previously moved for summary judgment with respect to Experi–Metal's claim that the bank, pursuant to Michigan Compiled Laws sections 440.4702 and .4703, bears the risk of loss for the unauthorized wire transfer orders the criminal executed on January 22, 2009. Michigan adopted these provisions from sections 4A–202 and 4A–203 of the Uniform Commercial Code ("U.C.C."). This Court summarized the application of these sections in its opinion and order denying Comerica's motion:

> Pursuant to Section 440.4702, wire transfer orders are effective as orders of the customer, even though the customer did not authorize the payment orders, if: (1) the bank and customer agreed that the authenticity of payment orders would be verified pursuant to a security procedure; (2) the security procedure is commercially reasonable; and (3) the bank proves that it accepted the orders in good faith and in compliance with the security

> procedure and any written agreement or instruction of the customer. Mich. Comp. Laws § 440.4702(2).
>
> Even if these conditions are satisfied, the risk of loss nevertheless may shift to the bank if "the person committing the fraud did not obtain the confidential information [facilitating the breach of the security procedure] from an agent or former agent of the customer or from a source controlled by the customer ...." U.C.C. § 4A–203 (1)(b), cmt. 5; Mich. Comp. Laws § 440.4703(1)(b).
>
> (7/8/10 Op. and Order at 7–8.)

In that opinion and order, this Court found that the person(s) who committed the fraud against Experi–Metal on January 22, 2009, obtained Experi–Metal's confidential information that enabled the breach from an agent of Experi–Metal and that "[s]ection 440.4702, therefore is determinative of which party is responsible for the loss at issue in this case ...." (*Id.* at 8.) As to the criteria that must be satisfied under section 440.4702 to hold wire transfer orders effective as orders of the customer, the Court found no genuine issue of material fact that Comerica and Experi–Metal agreed that the authenticity of payment orders would be verified pursuant to a security procedure and that Comerica's security procedure was commercially reasonable. (*Id.* at 12.) The Court denied Comerica's motion, however, because it found genuine issues of material fact related to two issues:

> ***2** (1) whether Experi–Metal's employee, whose confidential information enabled the criminals to facilitate the fraudulent wire transfer orders, was authorized to initiate electronic wire transfer orders on behalf of the company and, therefore, whether Comerica complied with its security procedure when it accepted wire transfer orders executed with the employee's confidential information; and
>
> (2) whether Comerica acted in "good faith" when it accepted the orders.
>
> (*Id.* at 3 n. 2, 13, 15–16.)

The parties therefore presented evidence relevant to these issues during the six-day bench trial in this matter.

On February 2 and 3, 2011, after the bench trial concluded, the parties submitted proposed findings of fact and conclusions of law. (Docs.60, 62.) On February 17, 2011, Experi–Metal also filed a "supplemental brief" addressing the "good faith" standard articulated in the U.C.C. and the cases Comerica cites with respect to that standard. (Doc. 64.) Comerica responded to Experi–Metal's supplemental brief on February 22, 2011, arguing in part that it is unnecessary, unjustified, and unauthorized. (Doc. 65.) This Court neither requested nor needed additional argument to aid it in interpreting the cases the parties cited as relevant to the U.C.C.'s "good-faith" standard. It, therefore, is disregarding Experi–Metal's supplemental pleading and the arguments Comerica made in response thereto.

II. Findings of Fact

A. The Parties and Their Employees

Experi–Metal is a custom metal fabricating company, supplying stampings primarily to the automotive industry. (Compl. ¶ 4; 1/21/11 Trial Tr. at 167.) Experi–Metal is incorporated in Michigan and maintains its principal place of business in Macomb County, Michigan. (Compl.¶ 1.) Valiena Allison is Experi–Metal's president and chief executive officer. (1/21/11 Trial Tr. at 166.) Keith Maslowski is its controller. (1/20/11 Trial Tr. at 9.) Both individuals testified at trial.

Comerica is a Texas corporation, with its principal place of business in Dallas, Texas. (Notice of Removal at 1–2.) Based on total assets, Comerica ranks thirty-first among United States banks. (Trial Ex. 116.) The following Comerica employees testified at trial: Debra Nosanchuk, Claudia Cassa, Milverta Ruff, Denise Ling, Rita Pniewski, Connie

Jernigan, Shawn Murphy, Cathy Davis, Kenneth Scott Vowels, Anne Goldman, and Brenda Paige.

B. Banking Agreements, Establishing Experi–Metal's Online Banking Accounts, and Use of the Wire Transfer Service

Experi–Metal began banking with Comerica in September 2000, when Experi–Metal's loan officer at Huntington Bank, Claudia Cassa, moved to Comerica. On November 21, 2003, Ms. Allison, as Experi–Metal's president, signed a "Treasury Management Services Agreement" to gain "Funds Transfer services" through Comerica's NetVision Wire Transfer service. (Trial Ex. 1.) These services enable customers to "send payment order(s) or receive incoming funds transfers" from their Comerica account(s) through the Internet. (*Id.*) "Treasury Management" refers to the group at Comerica responsible for the bank's Internet or online banking system. (1/19/11 Trial Tr. at 40.)

*3 The Treasury Management Services Agreement is governed by the Comerica Treasury Management Services Master Agreement ("Master Agreement"), published August 2002, "and any applicable implementation documents and user guides as such documents are amended from time to time." (Trial Ex. 1.) Under the terms of the Treasury Management Services Agreement, Experi–Metal agreed to provide Comerica "with correct and timely Service implementation information as requested by [Comerica]." (*Id.* ¶ 1.) Relatedly, the Master Agreement states at paragraph 3(c) of Section I:

> Customer agrees to execute, in a form and content satisfactory to Bank, any and all documents required by Bank to obtain and to continue to receive a Service(s). Such documents may include deposit account Signature Cards, Declarations, Authorizations, Service Agreements, implementation documents and updated financial statements as requested by Bank from time to time.
>
> (Trial Ex. 51 at Comerica01656.)

After the Treasury Management Services Agreement was signed, Ms. Allison provided Brenda Paige, a Comerica Treasury Management sales officer, information regarding Experi–Metal's "users" of the NetVision Wire Transfer service and the services or "modules" available to each user. (1/24/11 Trial Tr. at 141–42, 144.) The users identified were Ms. Allison and Keith Maslowski, Experi–Metal's controller. (*Id.* at 145.) Ms. Paige loaded that information onto Comerica's "Implementation Worksheet," which is used to set-up the service for the customer. (1/24/11 Trial Tr. at 141–42; Trial Ex. 3.) Ms. Allison and Mr. Maslowski are identified as User 1 and User 2, respectively, on the "User Profiles" Implementation Worksheet. (Trial Ex. 3 at Comerica003315.) "User Access" is set forth on the Implementation Worksheet and includes the electronic initiation of wire transfer payment orders, reflected as code "450" on the document. (*Id.* at Comerica003325; 1/24/11 Trial Tr. at 23–24.)

On the Implementation Worksheet, six Experi–Metal accounts with Comerica are identified as being accessible through the NetVision Wire Transfer service: (1) the Sweep Account; (2) General Account; (3) Employee Savings Account; (4) Tax Account; (5) Payroll Account; and (6) Merchant Account. (Trial Ex. 3.) The worksheet reflects that electronic wire transfer orders could be initiated only from Experi–Metal's Sweep Account and General Account. (*Id.*) Experi–Metal's Employee Savings Account was a "zero balance" account, meaning that Experi–Metal transferred funds to the account and then immediately used the funds to pay Experi–Metal's employees. (1/24/11 Trial Tr. at 94.)

At a later date, six personal accounts of Ms. Allison's family were made accessible through Comerica's NetVision Wire Transfer service. (Trial Tr. 1/19/11 at 53–54; Trial Ex. 4.) These personal accounts were identified as: (1) Valiena checking; (2) Joint; (3) Stock; (4) Garrick; (5) Skylar; and (6) Dan. (Trial Ex. 4.)

*4 On November 25, 2003, a few days after

Ms. Allison signed the Treasury Management Services Agreement for the NetVision Wire Transfer service, she also executed a "Contingency Authorizations and Security Procedures" form. (Trial Ex. 2.) Ms. Cassa explained to Ms. Allison that this form allows users to initiate wire transfer orders by telephone in the event the NetVision Wire Transfer service was not operating. (1/21/11 Trial Tr. at 185–86; 1/19/11 Trial Tr. at 48; 1/24/11 Trial Tr. at 38.) Ms. Allison and Mr. Maslowski are identified as "users" on the contingency form. (Trial Ex. 2.) Experi–Metal did not elect to require a call back to verify the authenticity of a payment order requested by phone when the online service was not available. (*Id.*) The form states that the "[c]ustomer understands that the Authorized User(s) in Section II [Ms. Allison and Mr. Maslowski] have no dollar limitations except to the extent that the wire exceeds the available balance in the account." (*Id.*)

Ms. Allison was identified as the administrative user for Experi–Metal's NetVision Wire Transfer service. (Trial Ex. 3 at Comerica003315.) This gave Ms. Allison the authority to control user access to the service and the various modules within the service. (Trial Ex. 52 at 19–20; Trial Ex. 53 at 32–33; 1/24/11 Trial Tr. at 20–21, 37–38.) In January 2004, Debra Nosanchuk, a Comerica Treasury Management administrator, visited Experi–Metal's offices to train Ms. Allison with respect to the NetVision Wire Transfer service and Ms. Allison's administrative controls within the service. (1/19/11 Trial Tr. at 44.)

During this on-site training, Ms Nosanchuk explained the purpose of each module to Ms. Allison and reviewed with her the Experi–Metal accounts accessible through the service. (1/19/11 Trial Tr. at 44.) Ms. Nosanchuk trained Ms. Allison on how to control "service assignments"—the modules to which users had access—and explained how Ms. Allison could grant or remove a user's access whenever she wanted. (*Id.* at 45.) Ms. Nosanchuk also reviewed with Ms. Allison any limitations established for the particular modules, such as whether there were dollar limits for any transactions and/or approver(s) required for transactions. (*Id.*) Experi–Metal did not elect to require an approver for wire transfer payment orders initiated through the service. (*Id.* at 46.) A user without administrative credentials cannot control service assignments (1/21/11 Trial Tr. at 98–99.) Ms. Allison operated the computer and took copious notes while Ms. Nosanchuk trained her. (1/19/11 Trial Tr. at 46.)

After Experi–Metal began using the NetVision Wire Transfer service, Mr. Maslowski initiated wire transfer payment orders through the service and he believed he was authorized to execute this function. (1/20/11 Trial Tr. at 30.) Specifically, Mr. Maslowski initiated at least one payment order for a wire transfer to "P & F Tool and Dye" in Nova Scotia, Canada in 2005. (*Id.* at 31.) Mr. Maslowski also contacted Comerica's Treasury Management group to set up wire templates. (*Id.; see also* Trial Ex. 10.)

***5** As a user of the NetVision Wire Transfer service, Mr. Maslowski additionally was authorized to conduct Automated Clearing House ("ACH") transactions online. (1/21/11 Trial Tr. at 193) ACH transactions, like wire transfers, are a method of making payments from and receiving funds into a customer's bank account(s). (1/24/11 Trial Tr. at 29.) However, unlike a wire transfer where the funds are moved immediately from the customer's account and usually reach the beneficiary within the same day, an ACH transaction may take several days to complete. (*Id.*)

On September 15, 2004, Comerica received a "Declaration and Agreement for Opening and Maintaining Deposit Account(s) and Treasury Management Services" ("Declaration") executed by Ms. Allison. (Trial Ex. 9.) Paragraph 3 of the Declaration states: "Any one (1) of the persons named in this section ("Authorized Signer") is authorized on behalf of Customer to: (a) enter contracts regarding the establishment of deposit accounts; and (b) make withdrawals or required transfers from such accounts in any manner or form the bank may make

available." (*Id.*) The Declaration further provides: "Transfer requests and withdrawals will be valid if ordered by (I) an Authorized Signer or (II) someone authorized to do so pursuant to the applicable deposit account contract or (III) any person or entity designated in any other agreement entered by Customer and Bank." (*Id.*) Ms. Allison, Allan J. Sharp (Experi–Metal's Vice President of Sales), and Gerald W. King (Experi–Metal's Vice President of Manufacturing) are identified as "Authorized Signers" in the Declaration. (*Id.*)

According to Ms. Allison, in May 2007, she discovered that Mr. Maslowski had the capacity to initiate electronic wire transfer payment orders. (1/24/11 Trial Tr. at 40, 70.) Ms. Allison testified that she wanted to be the only Experi–Metal employee capable of initiating wire transaction payment orders and, therefore, she contacted Ms. Cassa and instructed her to prepare whatever documents were necessary to limit that authority to her. (*Id.* at 70–71.) Experi–Metal identifies a "Global Wire Transfer Authorization and Security Procedures" document, executed by Ms. Allison on November 1, 2007, as the form Ms. Allison subsequently received from Ms. Cassa to effectuate her request. (*Id.* at 72; Trial Ex. 103.)

The Global Wire Transfer Authorization and Security Procedures document identifies Ms. Allison, only, as the initiator of wire transfer requests. (*Id.* Trial Ex. 103.) On page two, under the heading "Initiation of Wire Transfer Requests," the document states the following:

> Wire transfer requests will be taken by telephone at the number provided in the Global Funds Transfer User Guide. The caller must identify himself/herself and provide a PIN. If the PIN provided by the caller does not match that of an Initiator, Comerica will not accept the wire transfer request and will notify an authorized representative of the Customer.

***6** (*Id.*) According to this document, Comerica was required to confirm the authenticity of payment orders exceeding $250,000. (*Id.*)

In the e-mail by which the Global Wire Transfer Authorization and Security Procedures document was transmitted to Ms. Allison on November 1, Mary Wezner in Ms. Cassa's office wrote to Ms. Allison: "I will be processing your wire request today, but need you to fill out the attached form for any future wire transfers you request of us. We are being audited and we don't want to be lacking the attached documents with regards to wires being processed for you." (*Id.*)

A month later, on December 1, 2007, Ms. Allison executed a form entitled "Declaration for Entering Wire Transfer Agreements and Designation of Authorized Agents." (Trial Ex. 104.) Ms. Allison testified that Ms. Cassa had her complete this document because Ms. Allison was going on vacation and Ms. Cassa noted that there was no one at Experi–Metal authorized to execute wire transfer payment orders in her absence. (1/24/11 Trial Tr. at 75.) According to the document, the "Declaration applies to Wire Transfer Transactions" and provides:

> Any one (1) of the persons named in this section ("Authorized Agent") is authorized on behalf of this entity to (a) enter contracts regarding wire transfers; and (b) designate those persons who can request a wire transfer payment order, cancellation and/or change to payment orders in the name of this entity and who can designate the bank account of this entity that is to be charged for the amount of the requested payment orders and related charges and fees, whether or not such person(s) is/are also designated by this entity as an Authorized Signer of such designated account(s) ...

(*Id.*) Ms. Allison and Mr. King are listed on this document as Experi–Metal's "Authorized Agents." (*Id.*)

In April 2008, Comerica notified the administrative users for all online banking accounts that the

bank was switching its security process from digital certificates to "secure token technology." (Trial Ex. 21; 7/8/10 Op. and Order at 4.) Comerica thereafter sent the administrators a list of the users for their accounts who had been active for the last six months, user IDs, and a secure token for each user. (*Id.*) Comerica asked the administrators to notify Comerica if the registration for any user should be removed. (*Id.* at 5.) Ms. Allison, as Experi–Metal's administrative user, received this information from Comerica on April 25, 2008. (*Id.*) Ms. Allison and Mr. Maslowski were listed by Comerica as authorized users of the online service. (*Id.*) Ms. Allison thereafter gave Mr. Maslowski the secure token that Comerica provided for him. (1/24/11 Trial Tr. at 60.)

C. The Phishing Incident

During the morning of January 21, 2009, Comerica was alerted to phishing e-mails sent to its customers by a third-party attempting to lure the customers into providing their confidential identification information. (1/20/11 Trial Tr. at 88.) This was not the first time that Comerica's customers had been the target of such phishing attacks. (*See id.* at 115.) In fact, Comerica drafted a procedure to respond to fraudulent activity triggered by its customers responding to phishing e-mails. (Trial Ex. 38.)

*7 Mr. King, Experi–Metal's Vice President of Manufacturing, forwarded this phishing e-mail to Mr. Maslowski at 6:48 a.m. on January 22, 2009. (1/20/11 Trial Tr. at 12; Trial Ex. 39.) The e-mail instructed the recipient to click on an attached link to complete a "Comerica Business Connect Customer Form." (Trial Ex. 30.) At approximately 7:35 a.m., Mr. Maslowski clicked on the link and was directed to a website where he responded to a request for his confidential secure token identification, Treasury Management Web ID, and login information. (1/20/11 Trial Tr. at 13.) By doing so, Mr. Maslowski provided a third-party with immediate online access to Experi–Metal's Comerica bank accounts from which the individual began initiating wire transfer payment orders from Experi–Metal's Sweep Account—one of only two accounts from which online wire transfer orders were authorized.

Between 7:30 a.m. and 2:02 p.m., ninety-three fraudulent payment orders totaling $1,901,269.00 were executed using Mr. Maslowski's user information. (Trial Ex. 44.) The majority of these payment orders were directed to accounts at banks in destinations where most cyber-crime has been traced (i.e. Russia and Estonia). (*Id.*; 1/25/11 Trial Tr. at 192.) Before the fraudulent wire transfer activity started, Experi–Metal had $229,586.56 in its Sweep Account and $316,398.05 in its General Account. (Trial Ex. 45.)

To facilitate the fraud, the criminal transferred all of the money in Experi–Metal's General Account to its Sweep Account. (*See* Trail Ex. 44.) The criminal also transferred existing and non-existing funds from the company's other accounts and the Allison family's personal accounts to the Sweep Account. (*Id.*) In total, between 7:40 a.m. and 1:59 p.m., the criminal executed twenty "book transfers" totaling more than $5.6 million. (*Id.*) Only three of the book transfers were rejected by Comerica due to "[f]unds not available." (*Id.*) Yet most of the book transfers ($5 million) were made from Experi–Metal's Employee Savings Account which had no funds at the start of the day—thereby creating an overdraft of $5 million in the account. (Trial Ex. 45; 1/21/11 Trial Tr. at 105–06.)

At approximately 11:30 a.m., Milverta Ruff, a Comerica Treasury Management investigation analyst, received a telephone call from J.P. Morgan Chase reporting six suspicious wire transfers. (1/19/11 Trial Tr. at 117.) In response, Ms. Ruff printed out information related to the suspicious transactions, which involved funds transferred from Experi–Metal's Sweep Account, through J.P. Morgan Chase, to the accounts of beneficiaries at Alfa–Bank in Moscow, Russia. (*Id.* at 121–22.) At 11:39 a.m., Ms. Ruff called Comerica's Treasury Management Customer Relations Center to identify the representative who handles Experi–Metal's ac-

counts. (*Id.* at 122.) Ms. Ruff was directed to Denise Ling, a Treasury Management Relations Specialist. (*Id.*) Ms. Ruff spoke with Ms. Ling for approximately five minutes over the telephone, during which time Ms. Ruff described the suspicious wire transfers and asked Ms. Ling to contact Experi–Metal to determine whether the company had initiated the payment orders. (*Id.* at 123–24.)

***8** After speaking with Ms. Ruff, Ms. Ling printed a report of all wire transfer activity from Experi–Metal's accounts that day so she could answer any questions the company might ask when she called. (1/19/11 Trial Tr. at 179.) The report printed at 11:47 a.m. (Trial Ex. 32.) Ms. Ling then called Experi–Metal to inquire about the wire transfer activity and learned from Ms. Allison that the company had not processed any wire transfer payment orders that day. (1/19/11 Trial Tr. at 181.) Ms. Ling reported the fraudulent wire activity to her supervisor, Rita Pniewski, sometime between 11:47 a.m. (when Ms. Ling printed her report) and 11:59 a.m. (when Ms. Pniewski reported the fraud to Comerica's fraud group). (1/19/11 Trial Tr. at 180; 1/20/11 Trial Tr. at 94–95; Trial Ex. 33.)

At 12:04 p.m., Ms. Ling sent an e-mail to Ms. Ruff in Comerica's wire room, which she copied to Comerica's "escalation team" (i.e. Ms. Pniewski and Annie Goldman), advising that the wire transfer activity was not legitimate, to recall all processed wires, and stop all future activity. (1/19/11 Trial Tr. at 181; Trial Ex. 35.) Ms. Ling attached to her e-mail the report she had generated of the already processed wire activity that day. (1/19/11 Trial Tr. at 182; Trial Ex. 35.) Ms. Ling phoned Ms. Ruff sometime between 12:04 and 12:15 p.m. to inform Ms. Ruff that she had sent the e-mail. (1/19/11 Trial Tr. at 124.)

At 12:24 p.m., Ms. Ruff flagged Experi–Metal's accounts to hold wire transfer payment orders for review before processing. (*Id.*) At 12:27 p.m., an operator approved Ms. Ruff's action which should have stopped all wire payment orders in the queue. (*Id.* at 126–27.) Ms. Ruff then began the process of recalling the previously processed wire transfer orders. (*Id.* at 127.)

In the meantime, following Comerica's procedure in response to unauthorized wire transfer activity (*see* Trial Ex. 38), Ms. Pniewski contacted Connie Jernigan to disable Experi–Metal's user identifications from the online banking system and to "kill" the user's session in which the fraudulent transfers were being executed. (1/20/11 Trial Tr. at 91–92, 183.) Ms. Jernigan is a Quality Risk Manager in Comerica's Electronic Data Management group. (1/20/11 Trial Tr. at 167.) At 12:25 p.m., Ms. Jernigan disabled all user identifications for Experi–Metal's accounts by changing the passwords of Experi–Metal's users and "the entablement date." (*Id.* at 168; Trial Ex. 42.) This prevented anyone from accessing the wire transfer service using the identification of any Experi–Metal user. (1/20/11 Trial Tr. at 168.) Ms. Jernigan's actions, however, did not preclude any users already logged into the system from continuing to conduct online activity and thus the criminal remained capable of initiating additional wire transfer payment orders after 12:25 p.m. (*Id.* at 184.) Ms. Jernigan subsequently was informed of the continued wire transfer activity and eventually "killed" the session at 2:05 p.m. (*Id.;* Trial Ex. 42.)

***9** Between 12:24 p.m.—when Ms. Ruff flagged Experi–Metal's accounts—and 2:05 p.m.—when Ms. Jernigan finally killed the session and kicked the criminal out of the service, fifteen additional fraudulent wire transfer orders were initiated. (Trial Ex. 44.) Comerica cancelled or recovered the funds for all but one of those fifteen transactions. (*Id.;* Trial Ex. 46.) An employee in Comerica's wire room released a wire transfer entered at 1:08 p.m. for $49,300 and the funds were never recovered. (*Id.;* 1/21/11 Trial Tr. at 61–62.)

During the approximately six and a half hours that the criminal had access to Experi–Metal's accounts via Comerica's online service, wire transfers totaling $1,901.269.00 were executed. (Trial Exs. 44–46.) Comerica recovered all but $561,399. (Jt.

Pretrial Order at 6.)

III. Conclusions

A. Whether Keith Maslowski Was Authorized to Initiate Wire Transfer Payment Orders Through Comerica's Wire Transfer Service on January 22, 2009

The evidence establishes that Mr. Maslowski was authorized to initiate wire transfer payment orders on the date of the phishing incident. There is no single writing signed, submitted, or prepared by Experi–Metal expressly authorizing Mr. Maslowski to initiate electronic wire transfer payment orders. Nevertheless, Experi–Metal does not dispute that Mr. Maslowski was authorized to conduct ACH transfers using Comerica's online service and there was no writing signed, submitted, or prepared by Experi–Metal granting him that authority.

Pursuant to the Declarations Ms. Allison signed on Experi–Metal's behalf on September 15, 2004 and December 1, 2007, Ms. Allison was authorized to enter agreements on Experi–Metal's behalf with respect to the company's accounts with the bank and to designate those individuals who could withdraw and transfer funds from those accounts. As Experi–Metal's president, Ms. Allison entered into the Treasury Management Services Agreement for Comerica's NetVision Wire Transfer service, which was governed by the Comerica Treasury Management Services Master Agreement. Both agreements provide that Experi–Metal "agrees to execute, *in a form and content satisfactory to Bank,* any and all documents required by Bank to obtain and to continue to receive a Service(s)." (Trial Ex. 51 § 1, ¶ 3(c) (emphasis added); *see also* Trial Ex. 1 ¶ 1.)

Ms. Allison—again, designated by Experi–Metal as an Authorized Agent and Authorized Signer with respect to its accounts with Comerica—provided the implementation information to Ms. Paige, identifying Ms. Allison and Mr. Maslowski as users of the NetVision Wire Transfer service and Ms. Allison as the administrative user. Within days of executing the Treasury Management Services Agreement for the Comerica NetVision Wire Transfer service, Ms. Allison also signed a "contingency" form identifying herself and Mr. Maslowski as "users" authorized to initiate wire transfer payment orders by telephone *in the event that* the online service was unavailable.

***10** Ms. Nosanchuk trained Ms. Allison in person with respect to the NetVision Wire Transfer service, which included reviewing on the computer each module and describing the users' capabilities therein and explaining how to make changes to the rights assigned to the users. As demonstrated during her testimony, Ms. Allison is an educated, savvy, and detail-oriented business person, and the Court does not find credible her claimed fear of her administrative capabilities within the system or her claim that she did not know until some time in early 2007 that Mr. Maslowski was authorized to initiate online wire transfer payment orders. As Ms. Nosanchuk demonstrated, the administrative user functions within the service are not complex and disabling a user's access to a module requires one simple click of the mouse. (1/24/11 Trial Tr. at 20.)

Also the Court finds it difficult to accept Ms. Allison's assertion that she discovered Mr. Maslowski's electronic wire transfer capability in May 2007, that she asked Ms. Cassa several months later to prepare any documents necessary to remove his authority, and that she believed the documents she signed in November and December 2007 effectuated that change. During her testimony, Ms. Allison stressed how important it was to her that Mr. Maslowski's authority be removed (1/21/11 Trial Tr. at 202); however, she had no explanation for why she waited several months to make the request. The documents Ms. Allison signed in November and December 2007 are not Treasury Management documents and there is nothing within the documents suggesting that they relate to the NetVision Wire Transfer service. Furthermore, Ms. Cassa lacked the authority to make changes related to the

NetVision Wire Transfer service. (1/19/11 Trial Tr. at 86, 88.) Therefore, whenever one of her customers had a question or needed something related to the NetVision Wire Transfer service, Ms. Cassa directed them to the Treasury Management department. (*Id.* at 80–83, 88.)

What the evidence instead suggests is that sometime around November 1, 2007, Ms. Allison attempted to initiate a wire transfer payment order by telephone when the online service was functioning and Comerica lacked documentation authorizing the transaction under those circumstances. This is supported by the language of the e-mail sent by Ms. Cassa's office to Ms. Allison to which the subsequently executed document was attached. It is further suggested by the language of the document Ms. Allison signed, which clearly indicates that it authorizes wire transfer requests initiated by telephone, only. The document neither refers to the removal of any user's authority, the NetVision Wire Transfer service, nor wire transfer requests initiated by any method other than by telephone.

The Declaration subsequently signed by Ms. Allison on December 1, 2007, also does not remove the authority of any user to conduct wire transfer payment orders through Comerica's online service. The document does not even mention the online service. The fact that the form identifies only Ms. Allison and Mr. King does not suggest that Mr. Maslowski was not authorized to initiate wire transfer payment orders through the online service. Instead, the document identifies Ms. Allison and Mr. King as the only agents authorized to "enter into a wire transfer agreement and who *can designate those that are authorized to give wire transfer payment orders* ...." (Trial Ex. 18 (emphasis added).)

***11** Finally, when it was discovered that the criminal initiated the fraudulent wire transfer payment orders using Mr. Maslowski's online identification information, Ms. Allison never asked how this was possible given that she believed she had removed Mr. Maslowski's authority to initiate electronic wire transfer orders. Ms. Allison neither asked anyone at Comerica this question before this case was filed, nor did she raise it in the statement she provided to the FBI when the incident was investigated. (1/19/11 Trial Tr. at 90, 185; 1/21/11 Trial Tr. at 95–96; Trial Ex. 50.)

The Court finds that Mr. Maslowski was authorized to initiate wire transfer orders through Comerica's online service on January 22, 2009, and the Court concludes that Comerica complied with its security procedures when it accepted the wire transfer orders initiated with his user information on that date.

B. Whether Comerica Accepted the Payment Orders in "Good Faith"

Despite the above conclusion, the fraudulent wire transfer orders will not be effective as orders of Experi–Metal if Comerica did not accept the orders in "good faith," as that term is defined in the U.C.C. *See supra* at 2–3. What conduct is required of a bank to comply with the "good faith" requirement cannot be varied by the parties' agreement(s). *See* Mich. Comp. Laws § 440.4702(6). The parties agree that the burden falls upon Comerica to prove that it accepted the payment orders in good faith.

"Good faith" is defined as "honesty in fact *and* the observance of reasonable commercial standards of fair dealing." Mich. Comp. Laws § 440.4605(1)(f). The same definition of "good faith" appears in other articles of Michigan's version of the U.C.C. and the U.C.C. itself.[FN3] *See, e.g.*, U.C.C. §§ 1–201, 3–103.

> FN3. "When uniform laws such as the UCC have been adopted by several states, the courts of one state may refer to decisions from another state and may construe the statutes in accordance with the construction given by that state." *Yamaha Motor Corp., U.S.A. v. Tri–City Motor Sports, Inc.*, 171 Mich.App. 260, 270, 429 N.W.2d 871, 876 (1988). Additionally, "[t]he Official Comments appended to each section of the UCC, although lacking

> the force of law, are useful aids to interpretation and construction." *Id.* at 271, 429 N.W.2d at 876 (citations omitted). The Official Comments to the U.C.C. indicate that, except where expressly indicated, the obligation of "good faith" in all Articles of the U.C.C. is the same. *See* UCC § 1–201 cmt. 20. Therefore, cases interpreting "good faith" within the context of one provision are instructive in defining the term elsewhere.

The "honesty in fact" prong of the definition is subjective. *See, e.g., In re Jersey Tractor Trailer Training, Inc.*, 580 F.3d 147, 156 (3d Cir.2009); *Maine Family Fed. Credit Union v. Sun Life Assurance Co. of Canada*, 727 A.2d 335, 340 (Me.1999). It has been referred to as the "pure heart and empty head" standard. *Maine Family Fed. Credit Union*, 727 A.2d at 340. There is no suggestion in the record that Comerica's employees acted dishonestly in accepting the fraudulent wire transfer orders. The issue in this case is whether they acted in "observance of reasonable commercial standards of fair dealing."

This prong of the "good faith" definition is objective. *Id.* at 340; *In re Jersey Tractor Trailer Training*, 580 F.3d at 156. The Official Comments to the U.C.C. make clear that this objective standard should not be equated with a negligence test:

> Although fair dealing is a broad term that must be defined in context, it is clear that it is concerned with the fairness of conduct rather than the care with which an act is performed. Failure to exercise ordinary care in conducting a transaction is an entirely different concept than failure to deal fairly in conducting the transaction.

*12 U.C.C. § 1–201 cmt. 20. There is a paucity of cases and authority discussing this recently added prong of the "good faith" requirement. As far as this Court found, only one court, the Maine Supreme Court, has proposed an approach to address whether this prong has been met:

> The factfinder must ... determine, first, whether the conduct of the holder comported with industry or "commercial" standards applicable to the transaction and, second, whether those standards were reasonable standards intended to result in fair dealing. Each of those determinations must be made in the context of the transaction at hand.

Maine Family Fed. Credit Union, 727 A.2d at 343; *see also In re Jersey Tractor Trailer Training*, 580 F.3d at 157 (applying the Supreme Court of Maine's two-part test).

Experi–Metal presented the testimony of its expert, Jonathan Lance James, to demonstrate that Comerica failed to meet industry or commercial standards by accepting the fraudulent wire transfers at issue. Mr. James testified that industry standards required Comerica to engage in fraud scoring and fraud screening, which would have immediately stopped the wire transfers based on certain variables and risk factors. These variables and risk factors include, but are not limited to, the following: the limited prior wire transfer activity in Experi–Metal's accounts (only two transfers initiated in prior years, both in 2007); the length of Experi–Metal's prior online sessions compared to the criminal's session on January 22, 2009; the pace at which the payment orders were entered on January 22, 2009; the destinations of the wire transfers (Moscow, Estonia, and China); and the identities of the beneficiaries (individuals, many with Russian-sounding names). According to Mr. James, a "[m]ajority of the banks" have implemented monitoring systems to detect fraudulent activity.[FN4] (1/25/11 Trial Tr. at 186.)

> FN4. Even Paul Carrubba, Comerica's expert witness, acknowledged that "some banks" were moving to fraud monitoring systems as of January 2009. (1/25/11 Trial Tr. at 92.)

Mr. James failed to convince this Court, however, that on January 22, 2009, a bank had to provide fraud monitoring with respect to its com-

mercial customers to comport with "reasonable commercial standards of fair dealing." While the evidence suggests that the Federal Financial Institution Examination Council's Handbook provides guidance to banks with respect to its commercial customers, express security mechanisms outlined in the handbook are not mandatory for those customers. Mr. James was not specific as to which banks have adopted fraud monitoring. He identified by name only a few banks that have done so. However, and perhaps most importantly, he failed to inform the Court as to when a "majority of the banks" or even the few banks he named implemented fraud monitoring systems. No evidence was presented to the Court from which it can conclude that banks comparable in size to Comerica utilized fraud screening and fraud scoring as of the date of the incident at issue in this lawsuit.

The lack of such evidence, however, does not lead the Court to conclude that Comerica should prevail in this lawsuit. As discussed above, Comerica bears the burden of demonstrating that it accepted the wire transfer payment orders in good faith. As also set forth earlier, the parties cannot vary by agreement what satisfies the "good faith" standard. In other words, if "reasonable commercial standards of fair dealing" obligated Comerica to respond to the fraudulent wire transfer activity in a particular way and Comerica failed to observe those standards, it cannot demonstrate that it acted in good faith simply by showing that it was relieved of the obligations to adhere to any of those standards in its agreement(s) with Experi–Metal.

***13** In short, to prevail, Comerica had to present evidence conveying the reasonable commercial standards of fair dealing applicable to a bank's response to an incident like the one at issue here and to show, by a preponderance of the evidence, that its employees observed those standards in response to the criminal's phishing attack on January 22, 2009. This Court finds that where the burden falls is dispositive in this matter because Comerica failed to present evidence sufficient to satisfy its burden.

Comerica focuses almost exclusively on the subjective intent of its employees in arguing that it accepted the payment orders in good faith. As discussed earlier, however, the "good faith" requirement is no longer satisfied simply by meeting the "pure heart and empty head" standard. Thus contrary to Comerica's assertion in its proposed conclusions of law, "whether Comerica acted in good faith" *does not* simply "hinge[ ] upon the bank's motives when it accepted the wire transfer payment orders." (Doc. 62 at 19.) Comerica was required to present evidence from which this Court could determine what the "reasonable commercial standards of fair dealing" are for a bank responding to a phishing incident such as the one at issue and thus whether Comerica acted in observance of those standards. Comerica presented no such evidence and thus it has not satisfied its burden of showing that it satisfied the objective prong of the "good faith" requirement.

Comerica did attempt to demonstrate that Comerica shut down the fraudulent wire activity within a reasonable time after receiving J.P. Morgan Chase's alert of suspicious activity. Comerica's expert, Paul Carrubba, opined that Comerica's employees responded in a reasonable amount of time. (1/25/11 Trial Tr. at 16.) However, in this Court's view, Mr. Carrubba is not qualified to provide an expert opinion with respect to the reasonable commercial standards of fair dealing applicable to banks responding to phishing incidents due to his admitted lack of experience as a banker with Internet banking systems, specifically online wire transfer activity and "phishing" issues. (*See* 1/24/11 Trial Tr. at 154–56; 1/25/11 Trial Tr. at 17.) Thus Mr. Carrubba also lacks the expertise to advise the Court as to whether Comerica's failure to detect the suspicious and unusual online activity in Experi–Metal's accounts conformed to reasonable commercial standards of fair dealing.

Mr. Carrubba is qualified to provide his expert opinion as to whether Experi–Metal's agreements

with Comerica allowed overdrafts (he answered that they did) and whether there is an industry standard prohibiting banks from paying overdrafts on an account (he knew of no standard). (*See* 1/24/11 Trial Tr. at 182–83.) The evidence undoubtedly reflects that Experi–Metal conducted transactions approximately three to four times a year that resulted in overdrafts in its accounts. (1/19/11 Trial Tr. at 88–99, 108.) Nevertheless, neither Mr. Carrubba's testimony nor the evidence informed the Court of whether a bank engages in fair dealing when it allows overdrafts totaling *$5 million* from a single account that usually has a zero balance, particularly where the ten transactions causing the overdrafts were entered repetitively (many in less than a minute of each other) and during one online session. (*See* Trial Ex. 44.) Reasonable commercial standards of fair dealing are not demonstrated by evidence that Comerica approved one transaction in May 2004, resulting in an overdraft of $250,000 in Experi–Metal's General Account. (*See* Trial Ex. 8.)

IV. Conclusion

*14 On January 22, 2009, Mr. Maslowski was authorized to initiate wire payment orders on behalf of Experi–Metal via Comerica's NetVision Wire Transfer service. On that same date, Mr. Maslowski received a phishing e-mail targeting Comerica's customers. Mr. Maslowski fell into the fraudster's net. He clicked on the link in the phishing e-mail, and was directed to a webpage where he was asked to enter his confidential user information. Mr Maslowski complied, thereby giving the criminal the key to the bank—or more specifically, access to Experi–Metal's accounts via Comerica's online banking service.

Over the next several hours, the criminal initiated 97 wire transfer payment orders from Experi–Metal's Sweep Account, totaling more than $1.9 million. There are a number of considerations relevant to whether Comerica acted in good faith with respect to this incident: the volume and frequency of the payment orders and the book transfers that enabled the criminal to fund those orders; the $5 million overdraft created by those book transfers in what is regularly a zero balance account; Experi–Metal's limited prior wire activity; the destinations and beneficiaries of the funds; and Comerica's knowledge of prior and the current phishing attempts. This trier of fact is inclined to find that a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier. Comerica fails to present evidence from which this Court could find otherwise.

Accordingly, a Judgment consistent with this Bench Opinion shall be prepared by Experi–Metal's counsel and, after obtaining approval as to form by Comerica's counsel, submitted for entry by this Court.

E.D.Mich.,2011.
Experi-Metal, Inc. v. Comerica Bank
Not Reported in F.Supp.2d, 2011 WL 2433383 (E.D.Mich.), 74 UCC Rep.Serv.2d 899

END OF DOCUMENT