UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

EXPERI-METAL, INC.,

Plaintiff,

v.

Case No. 09-14890
Honorable Patrick J. Duggan

COMERICA BANK,

Defendant.
_____/

BENCH OPINION

This matter arises from a "phishing"[1] 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

[1]"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.

transfers falls upon Comerica pursuant to Michigan Compiled Laws sections 440.4601-4957.[2] This decision follows a bench trial with respect to Experi-Metal's claim, held on January 19-26, 2011.

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).

---

[2]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.

(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:

> (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.)

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.)

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.)

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.

(*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.)

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 accounts. (*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.)

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.)

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.

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).)

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.[3] *See, e.g.*, U.C.C. §§ 1-201, 3-103.

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

[3]"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.

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.

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.[4] (1/25/11 Trial Tr. at 186.)

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

[4]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.)

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.

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

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.

Dated:June 13, 2011

s/PATRICK J. DUGGAN
UNITED STATES DISTRICT JUDGE

Copies to:
Richard B. Tomlinson, Esq.
Daniel R. Boynton, Esq.
Joseph W. Thomas, Esq.
Todd A. Holleman, Esq.
Lara Lenzotti Kapalla, Esq.