UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

EXPERI-METAL INC.,
a Michigan corporation,

Plaintiff,

vs.

Case No. 2:09-cv-14890
Hon. Patrick J. Duggan

COMERICA BANK,

Defendant.

Richard B. Tomlinson (P27604)
Daniel R. Boynton (P 30359)
Joseph W. Thomas (P33226)
DRIGGERS, SCHULTZ & HERBST, P.C.
Attorneys for Plaintiff
2600 West Big Beaver Road, Suite 550
Troy, MI 48084
Telephone: 248.649.6000
Facsimile: 248.649.6442
rtomlinson@driggersschultz.com

Todd A. Holleman (P57699)
Lara Lenzotti Kapalla (P67667)
MILLER, CANFIELD PADDOCK AND
STONE, PLC
Attorneys for Defendant
150 W. Jefferson, Suite 2500
Detroit, MI 48226
Telephone: 313.963.7420
holleman@millercanfield.com
kapalla@maillercanfield.com

PLAINTIFF'S PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW

I. PROPOSED FINDINGS OF FACT

A. Events of January 22, 2009

1. On January 22, 2009, Keith Maslowski received what looked to him like a normal email which indicated it was from Comerica (Exhibit 109).[1]

2. The email looked to Maslowski to be like the emails that he had received over the years from Comerica in connection with renewing digital certificates (Exhibits 110, 111, 112).

3. Like the earlier emails that he had received from Comerica, the email on January 22, 2009 directed Maslowski to click on a website indicated in the email.

4. Keith Maslowski clicked on the website which looked exactly like the Comerica websites which he had been directed to over the years.

5. When he got to the website on January 22, 2009, he entered his log in and password and whatever confidential banking information was requested, similar to what he had done in the past, in responding to Comerica's emails.

6. After providing the information, unknown and unauthorized third parties obtained Maslowski's information, logged into Comerica's on line banking site, and began using TMConnect Web Wire Transfer Service to make 93 wire transfers out of Experi-Metal's accounts, sending the funds to various individual accounts in Russia, Estonia, China, Scotland and some domestic accounts.

7. Experi-Metal had not initiated any wire transfers since June of 2007.

B. Keith Maslowski was not authorized to initiate electronic wire transfers on behalf of Experi-Metal as of January 22, 2009.

1. On November 21, 2003, Experi-Metal's President, Valiena A. Allison, signed an Agreement with Comerica "to send payment orders" using Comerica's NetVision Wire Transfer Service – i.e., "Treasury Management Services Agreement Comerica NetVision Wire Transfer ("Net Vision Agreement")." (Exhibit 1).

2. Under the NetVision Agreement Experi-Metal agreed that the service provided by Comerica would be governed by the Comerica Treasury Management Services Master Agreement (August, 2002) and any

[1] References are to Trial Exhibit Numbers. Defendant's Exhibits are Exhibits 1-61. Plaintiff's Exhibits were referred to as Exhibits 101 through 170 during the trial.

applicable implementation documents and user guides as such documents are amended from time to time.

3. The Comerica Treasury Management Services Master Agreement (August, 2002) ("Master Agreement") (Exhibit 51), was prepared by Comerica.

4. Under the Master Agreement (August, 2002), Paragraph 3 outlined the requirements for submission of information and documents.

5. Paragraph 3(c) of the Master Agreement provided "Prior to utilizing any service, Customer shall furnish Bank with documentation naming Customer's employees, agents, and third party vendors hired by Customer, to perform any of the duties required by Customer under this Agreement and which names those who are authorized to act on behalf of Customer with respect to the Service." (Relevant portions of Exhibit 51 are attached).

6. On November 21, 2003, at the time that she signed the NetVision Agreement, Experi-Metal's President, Valiena A. Allison, signed an agreement – "Treasury Management Services Implementation Worksheet Comerica NetVision – Contingency Authorizations and Security Procedures" (Contingency Authorization and Security Procedures Agreement) (Exhibit 2) and provided that documentation to Comerica.

7. Under the Contingency Authorizations and Security Procedures Agreement, Experi-Metal authorized Keith Maslowski to initiate wire transfers by telephone in the event that the NetVision Wire Transfer Service was unavailable.

8. On or about December 5, 2003, Brenda J. Paige, a Comerica employee, prepared an internal Comerica document entitled "Treasury Management Services – Implementation Worksheet" (Implementation Worksheet) relating to Comerica NetVision (Exhibit 3).

9. Ms. Paige received some information from Experi-Metal's President, Valiena A. Allison, when Ms. Paige was preparing the Implementation Worksheet.

10. The Implementation Worksheet was an internal worksheet prepared by Comerica and was never provided to or shared with Experi-Metal and Experi-Metal never saw, signed or confirmed the document.

11. Experi-Metal's President, Valiena A. Allison, never advised Brenda Paige that Keith Maslowski was authorized to initiate electronic wire transfers on behalf of Experi-Metal.

12. Experi-Metal never furnished Comerica with documentation which named Keith Maslowski as someone who was authorized to initiate electronic wire transfers on behalf of Experi-Metal.

13. The NetVision Agreement (Exhibit 1) was not documentation by which Experi-Metal named Keith Maslowski as someone who was authorized to initiate electronic wire transfers on behalf of Experi-Metal.

14. The Implementation Worksheet (Exhibit 3) was not documentation furnished by Experi-Metal to Comerica which named Keith Maslowski as someone who was authorized to initiate electronic wire transfers on behalf of Experi-Metal.

15. Experi-Metal never furnished Comerica with documentation naming Keith Maslowski as someone who was authorized to initiate electronic wire transfers on behalf of Experi-Metal as of January 22, 2009 as required in Paragraph 3(c) of the Treasury Master Agreement.

16. Since Comerica prepared the Treasury Master Agreement, the agreement is to be construed most strictly against Comerica.

17. Valiena A. Allison discovered in 2007 that Mr. Maslowski was able to initiate electronic wire transfers through NetVision.

18. Valiena A. Allison advised Experi-Metal's account officer at Comerica, Claudia Cassa (Vice President), in October of 2007 that Mr. Maslowski should not be authorized to initiate any wire transfers on behalf of Experi-Metal and advised her that Valiena A. Allison would be the only person authorized to initiate wire transfers on behalf of Experi-Metal.

19. Valiena A. Allison asked Cassa to prepare all of the documents necessary to arrange that Valiena A. Allison would be the only person authorized to initiate wire transfers on behalf of Experi-Metal.

20. Valiena A. Allison advised Cassa that she still wanted Keith Maslowski to have access to Experi-Metal's banking information on line, and to initiate ACH transfers, but that she just did not want him to be able to initiate wire transfers, either electronically or by telephone.

21. Claudia Cassa advised Allison that she would send her all of the necessary paperwork so that Allison would be the only person authorized to initiate wire transfers on behalf of Experi-Metal.

22. Claudia Cassa provided Valiena A. Allison with a document entitled "Global Wire Transfer Authorization and Security Procedure" naming

Valiena A. Allison as the only authorized wire transfer initiator on behalf of Experi-Metal (Exhibit 17).

23. M. E. Wezner, who worked in Ms. Cassa's office, forwarded Exhibit 17 to Valiena A. Allison and advised Allison by email that she needed to fill out the attached form "for any future wire transfers you request of us."

24. On November 1, 2007, Valiena A. Allison signed the Global Wire Transfer Authorization and Security Procedures Agreement with Comerica (Exhibit 17) and returned the document to Claudia Cassa.

25. Claudia Cassa received Exhibit 17 from Valiena A. Allison and advised Allison that she was the only authorized initiator for wire transfers on behalf of Experi-Metal, either by phone or electronically as of November 1, 2007.

26. Claudia Cassa advised Valiena A. Allison in late November of 2007 that Experi-Metal should have two authorized wire transfer initiators because situations might arise where Ms. Allison was out of town or unavailable to initiate a wire and Experi-Metal might need to have a wire transfer initiated.

27. Valiena A. Allison agreed with Cassa, and told her that the only two authorized initiators of wire transfers would be Valiena A. Allison and Gerald King, as they were both owners of the Company.

28. Claudia Cassa advised Valiena A. Allison that she would send Allison all of the documents needed by Comerica to establish there would be two authorized initiators for wire transfers on behalf of Experi-Metal, Valiena A. Allison and Gerald King.

29. Cassa then provided documentation for Valiena A. Allison to sign authorizing herself and Gerald King as authorized signers and wire transfer initiators on behalf of Experi-Metal (Exhibits 18 and 19).

30. Valiena A. Allison signed Exhibits 18 and 19 on behalf of Experi-Metal on December 1, 2007 and sent them back to Claudia Cassa.

31. Claudia Cassa confirmed to Valiena A. Allison that Gerald King and Valiena A. Allison were the only two authorized initiators for wire transfers, electronic or otherwise, and that Valiena A. Allison did not have to take any other actions with respect to the authorization.

32. Valiena A. Allison relied on Cassa's confirmation and her reliance on the Bank's officer was reasonable.

33. Experi-Metal never modified or amended the Corporate Declaration which was signed by Valiena A. Allison on December 1, 2007 (Exhibit 18).

34. Neither Valiena A. Allison nor Gerald King ever designated Keith Maslowski as someone authorized to initiate wire transfer payment orders after the date of the Declaration signed by Valiena A. Allison on December 1, 2007 (Exhibit 18).

35. Keith Maslowski never initiated or attempted to initiate any wire transfers on behalf of Experi-Metal after May of 2007.

36. Comerica failed to comply with its security procedures when it accepted the wire transfer orders initiated with Maslowski's user information on January 22, 2009 as Maslowski was not an authorized wire transfer initiator on behalf of Experi-Metal.

37. Comerica failed to meet its burden of proof with regard to whether Maslowski was authorized to initiate electronic wire transfer orders using Comerica's on line service as of January 22, 2009. As a result, Comerica failed to meet its burden of proof as to whether Comerica complied with the security procedures and the written agreements between the parties when it accepted wire transfer orders initiated with Maslowski's user information on January 22, 2009.

C. Comerica failed to meet industry or commercial standards by accepting the wire transfers without monitoring the transfers for fraud scoring and fraud screening.

1. The Federal Financial Institution Examination Council ("FFIEC") is a formal interagency body empowered to prescribe principles, standards and report forms for the Federal examination of financial institutions by the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation (Exhibit 155).

2. The FFIEC promulgated its Information Technology Examination Handbook (the "FFIEC Handbook") in 2005 as its guidelines in this regard (Ex 155).

3. The E-Banking and Information Security Booklets of the FFIEC Handbook were introduced into evidence as part of Exhibit 155 (Exhibit 2 to Exhibit 155).

4. The FFIEC Handbook describes industry guidelines that apply to FDIC insured banks including Comerica.

5. As of April 1, 2008, Comerica represented on its website, “We safeguard information according to industry security standards and procedures (Exhibit 170, a copy of which is attached).

6. Comerica has also represented on its website “We are always monitoring our systems to prevent any problems that could compromise security or privacy.” (Exhibit 170).

7. The FFIEC Handbook, Information Security/Information Security Risk Assessment Booklet notes, “A well planned and executed security monitoring program is sound industry practice and should be based on an assessment of the risk of noncompliance or circumvention of the institution’s controls.” (Exhibit 155 FFIEC Handbook, Information Security/Information Security Risk Assessment, page 3 of 4). (Relevant portions of Exhibit 155 are attached).

8. The FFIEC Handbook Information Security/Security Controls Implementation notes that one of the weaknesses in token systems includes man-in-the-middle attacks. The weakness to man-in-the-middle attacks can be addressed through additional control mechanisms including the use of public key infrastructure and that behavioral authentication monitoring, or fraud screening and fraud scoring, are effective control mechanisms (FFIEC Handbook, Information Security/Security Controls Implementation, page 4 and 6 of 15, Exhibit 155).

9. Almost all of the 40 largest banks have adopted the guidelines of the FFIEC as industry standards and implemented monitoring systems, fraud scoring and fraud screening. Under these monitoring systems, readily available software is used to index historic transaction patterns and then compare those patterns against current activity through real time monitoring of current activity.

10. Under this type of monitoring, the monitoring system measures certain variables and risk factors including prior wire transfer activity, prior last log in checks, amounts involved in wire transactions, location of destination banks, destination bank accounts, session length on banking software, destination account name, destination bank locality, and IP address.

11. The monitoring software then assigns higher risk scores to activity that does not match the normal activities of the particular account involved and at a certain threshold the system alerts the bank to the unusual activity and freezes the activity to stop suspicious wires based on the fraud scoring and fraud screening.

12. The activity on January 22, 2009 relating to wire transfers from Experi-Metal accounts was so unusual and had so many obvious risk factors that

an elementary fraud scoring or fraud screening monitoring program would have been triggered with the first transaction and would have stopped all suspicious wire transfers.

13. Comerica did not use any monitoring, fraud screening or fraud scoring to measure the activity on Experi-Metal's accounts of January 22, 2009.

14. Comerica has failed to meet its burden of proof to show that Comerica acted in good faith in accepting the 93 wire transfer orders initiated with Maslowski's user information on January 22, 2009.

15. Comerica's conduct in accepting wire transfer orders without any monitoring, failed to comport with industry or commercial standards applicable to the transactions and those standards were reasonable standards intended to result in fair dealing.

16. The FFIEC Guidelines prescribing a well planned and executed security monitoring program as sound industry practice and the subsequent implementation of monitoring programs for fraud scoring and fraud screening by the 40 largest banks most of have established industry and commercial standards with respect to the acceptance of wire transfer orders.

17. Comerica's expert witness, Paul Carrubba, acknowledged that the FFIEC's Guidelines are applicable to Comerica.

18. Comerica's expert Witness, Paul Carrubba was unable to identify any of the 40 largest banks in the country that do not use monitoring, fraud scoring and fraud screening as of January 22, 2009.

19. Comerica's expert witness, Paul Carrubba, acknowledged that as of January 22, 2009, the FFIEC Guidelines requiring monitoring and fraud scoring and fraud screening, were becoming industry standards and monitoring programs were being utilized by a number of financial institutions.

20. Comerica did not accept the wire transfer payment orders in good faith and Comerica did not meet industry and commercial standards, because Comerica did not employ any type of monitoring system incorporating fraud scoring or fraud screening to detect suspicious or unusual activity prior to accepting the wire transfer orders.

21. By failing to have fraud scoring or fraud screening monitoring systems in place, Comerica did not address a known weakness to the man-in-the-middle attack which occurred in this case.

22. As a result of Comerica's failure to meet industry or commercial standards, the fraudsters were able to log in and make 93 wire transfers from Experi-Metal's bank accounts to many overseas locations over a seven hour period.

23. If Comerica had complied with industry and commercial standards, and had a monitoring system in place incorporating fraud scoring or fraud screening, Comerica would have quickly detected the fraudulent activity within the first transaction that occurred at 7:39 a.m.

24. Comerica's failure to implement a monitoring system with fraud scoring and fraud screening to detect suspicious or unusual activity shows that Comerica's conduct did not comport with industry or commercial standards applicable to the transactions, and the standards are reasonable standards intended to result in fair dealing.

D. Comerica failed to meet its own standards and failed to comport with industry or commercial standards when it failed to warn Experi-Metal of phishing emails being directed to customers on January 21, 2009, the day before the fraud occurred.

1. Comerica was well aware that phishing emails were being directed to its customers on the morning of January 21, 2009.

2. Despite the fact that Comerica was aware that phishing emails were being sent to its customers, Comerica failed to contact customers, including Experi-Metal in order to warn them of the fact that phishing emails were being sent to customers and the heightened risk of phishing attacks such as the attack in this case.

3. In April of 2008, when Comerica became aware of phishing emails being directed at Comerica's customers, Comerica complied with industry and commercial standards by warning its customers, including Experi-Metal.

4. Comerica failed to follow its own standards or the industry or commercial standards when it failed to warn Experi-Metal of phishing emails being directed to Comerica customers on January 21, 2009.

5. Comerica has failed to meet its burden to show that its actions in failing to warn its customers on January 21, 2009, were in good faith and in accordance with industry and commercial standards.

E. Comerica failed to act in accordance with the written agreements between the parties and failed to meet its own standards and failed to comport with industry or commercial standards in allowing corporate book transfers of $5 million from the zero balance employee savings account to the sweep account when there were no funds available in the employee savings account.

1. Experi-Metal had set up a zero balance employee savings account. Payroll funds would go into the account and then be immediately distributed out to direct deposit accounts that had been specified and directed by the employees.

2. The zero balance employee savings account did not have a balance of funds in it as the funds were immediately distributed out to the accounts directed by each of the employees.

3. On January 22, 2009, once the fraudsters got into the system, they made corporate book transfers of non-existent funds from the employee savings account to Experi-Metal's sweep account in order to fund the continued wire transfers being made by the fraudsters (Exhibit 137).

4. The fraudsters were able to complete $5 million of book transfers from the employee savings account to the sweep account, despite the fact that there were no funds in the employee savings account.

5. Under industry and commercial standards, banks do not permit the transfer of non-existent funds from one account to another account.

6. For years Comerica had followed a policy with Experi-Metal with respect electronic corporate book transfers that Comerica would not allow corporate book transfers from one account to another account, if the initial account had insufficient funds to make the transfer (Exhibits 107, 108).

7. In 2006 and 2007, Comerica had followed its own policy and rejected attempted book transfers from Experi-Metal from one account to another electronically because the transferring account had insufficient funds to make the transfer (Exhibits 107, 108).

8. Experi-Metal had never entered into an agreement with Comerica authorizing Keith Maslowski as an Authorized Signer for purposes of creating an overdraft under the agreements between the parties (Exhibit 119, Exhibit 54).

9. Comerica's acceptance of the corporate book transfer from the zero balance employee savings account based on Keith Maslowski's user information was in breach of the written agreements between the parties (Exhibit 119, Exhibit 54 and Exhibit 51).

10. If Comerica had not allowed the corporate book transfers from the zero balance employee savings account to the sweep account, Experi-Metal's sweep account would have been out of funds by 9:05 a.m. and no further wire transfers would have been permitted. Experi-Metal's losses would have been limited to $210,000 or less.

11. Comerica has failed to meet its burden of proof to show that allowing the $5 million in corporate book transfers was in good faith and in accordance with industry or commercial standards.

F. Comerica employees failed to follow simple directives and failed to comply with Comerica's internal standards and did not comport with industry or commercial standards in responding to the Experi-Metal phishing incidents.

1. Customers at Comerica were subject to over 30 phishing incidents during 2008 where fraudsters were able to send unauthorized wire transfers from Comerica's customers' accounts.

2. The evidence shows that by 8:18 a.m., six wires had been sent out of Experi-Metal's accounts to J.P. Morgan Chase, intended for ultimate delivery to personal bank accounts at Alpha Bank in Moscow, Russia for slightly more than $162,000.

3. J.P. Morgan Chase notified Comerica's wire room of these suspicious and possibly fraudulent wire transfers in the morning on January 22, 2009. Milverta Ruff, the Comerica employee in the wire room, testified initially, in her first deposition, that she had received a number of written FED requests, which were date and time stamped, from J.P. Morgan Chase notifying of the fraudulent and suspicious nature of the wire transfers that had been sent.

4. On January 22, 2009, at 11:18 a.m., Comerica received a written FED request from Bank of New York City, advising Comerica that a wire transfer payment directed through Bank of New York was considered to be fraudulent and urged Comerica to urgently confirm whether the wire transfer was correct or fraudulent (Exhibit 148). The wire room did not take any action with regard to the FED request and did not report it to Treasury Management.

5. Milverta Ruff initially testified that she took the written FED requests that she had received from J.P. Morgan Chase and had placed them in the written case files that she maintains for cases that she is involved with pursuant to Comerica policy.

6. Comerica's wire room followed a policy of printing out all FED requests that came into Comerica and placing those written FED requests in a delivery box. The wire room established a policy that the copies of the written FED requests in the delivery box would be picked up at 8:00 a.m., 11:00 a.m. and 2:00 p.m. each day and when the pickups were made, they would be distributed to the appropriate personnel.

7. The case files which were produced by Comerica did not contain the written FED requests that Milverta Ruff had testified to.

8. In her second deposition, Milverta Ruff testified that maybe she had not received written FED requests from J.P. Morgan Chase because she could not find them in the case files. She testified that she might have gotten some kind of phone call from J.P. Morgan Chase, but was unable to recall what time the call came in.

9. At trial, Ms. Ruff testified that she had received a phone call notification from J.P. Morgan Chase, warning of the suspicious and fraudulent wire transfers, and testified that the phone call must have come in at 11:30 a.m. in the morning. Milverta Ruff contacted the Treasury Management Department and reported the potential fraudulent and suspicious wire transfers at 11:39 in the morning.

10. Comerica (Denise Ling) first contacted Experi-Metal at 10:50 a.m. and asked if Experi-Metal had initiated any wire transfers. Allison advised Comerica that Experi-Metal had not initiated any wire transfers and that Comerica should not honor any further wire transfers or other electronic activity.

11. Rita Pniewski reported that the information given to the Treasury Management Department was that the wire room had received written FED requests from J.P. Morgan Chase reporting potentially fraudulent and suspicious wire transfers from Experi-Metal's accounts.

12. Between 11:49 and 11:54 a.m. the fraud was reported by Denise Ling to Rita Pniewski in the Treasury Management Department.

13. Ling had called Rita Pniewski, reported the fraud, and confirmed that she had already spoken with Experi-Metal five to ten minutes prior to 11:59 a.m.

14. As soon as the information was reported to Rita Pniewski, she contacted Connie Jernigan of the EDM Department in Comerica, and instructed her to disable the TMConnect Web and remove all access from the user as a result of the fraud.

15. Under Comerica policy, this required Jernigan to kill the session, so that anybody that was currently on line would be knocked off line immediately, a task which would take a minute or two to accomplish (Exhibits 130, 131 and 132).

16. The direction for Jernigan to disable the TMConnect Web was given by Rita Pniewski of the Treasury Management Department between 11:49 and 11:54 a.m.

17. Jernigan failed to follow the direction given by Pniewski, and failed to follow her own department's procedures, and failed to kill the session, allowing the fraudsters to continue making fraudulent wire transfers.

18. Jernigan failed to follow the directive or Comerica's procedures, and did not kill the session until 2:05 p.m. in the afternoon, more than two hours after having been directed to do so by Rita Pniewski.

19. As a result of her failure to follow Comerica's internal policies and standards, and commercial and industry standards, the fraudster successfully initiated 14 additional wire transfers from 11:49 a.m. to 2:05 p.m. and Experi-Metal lost an additional $137,407 related to wire transfers made after 11:49 a.m. which were not recovered by Comerica's recovery efforts (Exhibits 137, 136, and 140-152).

20. At about the same time, Denise Ling from Treasury Management, instructed Milverta Ruff by email at 12:04 p.m. (Exhibit 123) to immediately stop all future wires, and recall all of the wires that had been processed thus far.

21. In order to stop all future wires, Milverta Ruff was required to change one computer entry, which would take her approximately one minute to accomplish.

22. Milverta Ruff did not flag or stop all future wire transfers by making the computer entry until 12:24 p.m. (Exhibit 139).

23. After Milverta Ruff flagged all of Experi-Metal's wire transfers and stopped them, another employee from the wire room, Malinda, ignored the flags and the instructions regarding Experi-Metal's wire transfers, and at 1:24 p.m. accepted a wire transfer and paid out an additional $49,300 (Exhibit 140).

24. Comerica has failed to meet its burden of proof to show that the employees' failures detailed above were in good faith and in accordance with industry or commercial standards.

G. Comerica failed to follow the written instructions and written agreements of its customer.

1. Comerica failed to follow the written instructions of its customer, Experi-Metal, by failing to confirm the authenticity of a payment order in excess of $250,000 contrary to the provisions of Exhibit 17.

2. At 9:05 a.m., Comerica accepted a wire transfer on Experi-Metal's account in the amount of $297,000 without calling Allison at the phone number specified in the agreement (Exhibit 127).

H. Damages

1. As a result of the unauthorized wire transfers, Experi-Metal lost $561,399 (Exhibit 154).

II. CONCLUSIONS OF LAW

1. Whether the risk of loss for an unauthorized wire transfer order falls upon the bank or its customer is governed by Sections 440.4702 and 440.4703 of Michigan's Uniform Commercial Code – Funds Transfers which are adopted from Sections 4(A-202) and 4(A-203) of the Uniform Commercial Code (UCC).

2. 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. MCLA Section 440.4702(2).

3. Comerica's Treasury Management Services Master Agreement (August, 2002) governs the issue of Maslowski's authorization.

4. Comerica's Treasury Management Services Master Agreement (August, 2002) was drafted by Comerica and is to be construed against the drafter. *Performance Contracting, Inc. v Seaboard Sur. Co.*, 163 F3d 366, 370 (6th Cir. Mich 1998).

5. Paragraph 3(c) of Comerica's Treasury Management Services Master Agreement (August, 2002) provides in relevant part:

> "Prior to utilizing any service, Customer shall furnish Bank with documentation naming Customer's employees, agents and third party vendors hired by Customer to perform any of the duties required by Customer under this Agreement, and which names those who are authorized to act on behalf of Customer with respect to the service."

6. Experi-Metal never furnished Comerica with documentation which named Maslowski as being authorized to initiate electronic wire transfers on behalf of Experi-Metal.

7. Comerica has the burden of proof to demonstrate that Experi-Metal had authorized Keith Maslowski to initiate electronic wire transfers using Comerica's on line service as of January 22, 2009.

8. Comerica has the burden of proof to show that Comerica accepted the wire transfer orders in compliance with the security procedures and any written agreement between the parties, or instructions of the customer when it

accepted the wire transfer orders initiated with Maslowski's user information on January 22, 2009.

9. Comerica failed to show that Experi-Metal furnished Comerica with documentation naming Keith Maslowski as someone who was authorized to initiate electronic wire transfers on behalf of Experi-Metal as of January 22, 2009 as required in Paragraph 3(c) of the Treasury Master Agreement.

10. Comerica has failed to sustain its burden of proof to show that Maslowski was authorized by Experi-Metal to initiate electronic wire transfers as of January 22, 2009.

11. For this reason, Comerica has failed to sustain its burden of proof with respect to whether Comerica complied with the security procedures and any written agreement between the parties or instruction of Experi-Metal when it accepted the wire transfer orders initiated with Maslowski's user information on January 22, 2009.

12. Comerica has failed to meet its burden of proof to show that it accepted the wire transfer orders initiated with Maslowski's user information in "good faith."

13. Under Article 4A of the UCC, Experi-Metal has no burden to show that Comerica's actions were in bad faith.

14. Article 4A of the UCC defines "good faith" as "honesty in fact and the observance of reasonable commercial standards of fair dealing." MCLA 440.4605(1)(f).

15. The Third Circuit has explained that "good faith" as defined in the UCC, "has both a subjective prong – 'honesty in fact' and an objective prong – observance of 'reasonable standards of fair dealing.'" *In re, Jersey Tractor Trailer, Inc.,* 580 F3rd 147, 156 (3rd Cir, 2009).

16. The Court also adopted the "two-part test" established by the Maine Supreme Court for evaluating the second component: "First, whether the conduct…comported with industry or commercial standards applicable to the transactions and second, whether those standards were reasonable standards intended to result in fair dealing." *Id.,* at 157 (citing *Maine Family Fed. Credit v. Sun Life Assurance Co. of Canada,* 727 A2d 335, 343 (ME. 1999).

17. The industry and commercial standards that apply to Comerica in this case are established in part by the Federal Financial Institution Examination Council (FFIEC) which prescribes "uniform principles and standards for the Federal examination of financial institutions…the Council's actions

shall be designed to promote consistency in such examination and to ensure progressive and vigilant supervision." 12 USC Section 3301.

18. The *Graham-Leach-Bliley Act* of 1999 (GLB, 15 USC Section 6821 *et seq.* requires the Federal banking agencies to prescribe revisions to regulations and guidelines as may be necessary to ensure that financial institutions have policies and procedures and controls in place to deter and detect activities proscribed under 15 USC Section 6821.

19. The FFIEC has promulgated its Information Technology Examination Handbook (the FFIEC Handbook) which includes e-banking and information security booklets.

20. Comerica did not accept the wire transfers in good faith as Comerica did not meet industry standards because Comerica did not have monitoring systems with fraud scoring and fraud screening in place to detect unusual activity in Experi-Metal's accounts and did not address a known weakness to man-in-the-middle attacks as set forth in the FFIEC Guidelines.

21. Almost all of the 40 largest financial institutions (Comerica ranks 31st) have adopted the industry standards and implemented monitoring systems for fraud scoring and fraud screening which indexes historical transaction patterns and compares those patterns against current activity through monitoring of current activity. When a certain threshold is reached, the system alerts the bank to unusual activity, freezing the activity and stopping the suspect wire transfers.

22. If Comerica had complied with good faith and industry and commercial standards and implemented monitoring systems with fraud scoring or fraud screening, Comerica would have detected the fraudulent and suspicious activity at the first wire transaction on behalf of Experi-Metal based on the blatantly obvious risk factors present in the transaction. (A wire transfer by a customer who had not done a wire transfer in 19 months, a large wire transfer apparently directed to an individual beneficiary, directed to an account of a Moscow bank, different source IP address).

23. The rights and obligations of the parties under 4A(202) and 4A(203) of the Uniform Commercial Code may not be varied by agreement, 4A(202)(6), MCLA 440.4702(6) (except as provided in Section 4A(203)(1)(a) which is not relevant here). *Grabowski v Bank of Boston,* 997 F Supp 111 (Mass. 1997).

24. Comerica has failed to meet its burden of proof to show that Comerica acted in good faith in accepting the 93 wire transfer orders initiated with Maslowski's user information on January 22, 2009.

25. Comerica did not accept the wire transfer payment orders in good faith and did not meet industry and commercial standards because Comerica did not employ any monitoring system incorporating the fraud scoring or fraud screening to detect suspicious or unusual activity. The failure to have fraud scoring or fraud screening did not meet industry or commercial standards particularly when the banks are aware of their vulnerability to man-in-the-middle phishing attacks such as the one that occurred in this case as noted by the FFIEC.

26. Comerica's failure to implement a monitoring system with fraud scoring and fraud screening to detect suspicious or unusual activity demonstrates that Comerica did not comport with industry or commercial standards applicable to the transaction and those standards were reasonable standards intended to result in fair dealing.

27. Comerica has failed to meet its burden to show that its actions in failing to warn its customers on January 21, 2009 was in good faith and in accordance with industry and commercial standards as well as Comerica's own standards.

28. Comerica has failed to meet its burden of proof to show that allowing the $5 million in corporate book transfers from the zero balance employee savings account was in good faith and in accordance with industry or commercial standards, or in compliance with Comerica's own standards.

29. Comerica has failed to meet its burden of proof to show that the employees' failures to follow simple directives and failing to comply with Comerica's internal standards were in good faith and in accordance with industry or commercial standards.

30. Comerica failed to meet its burden of proving that it accepted the wire transfer orders in good faith and in compliance with industry or commercial standards applicable to wire transfer transactions and in compliance with any written agreements or instructions of the customer. MCLA 440.4702(2).

31. Reasonable commercial standards of fair dealing would not entail allowing 93 fraudulent wire transfers to be initiated from Experi-Metal's bank account, particularly with respect to a customer who had not made a single wire transfer in the 19 months prior to January 22, 2009. This is especially true where if Comerica had been acting in good faith, it would have been alerted to the fraudulent or suspicious nature of the wire transfers based on the unusual destinations where the money was being directed (such as Moscow, Estonia and China), particularly in light of Experi-Metal's limited wire transfer activities.

32. This is especially true in the present case where Comerica was on notice on January 21, 2009 that phishing emails were being directed to its customers and Comerica should have recognized a heightened sense of risk to its customers.

33. Comerica failed to meet its burden of proving that it accepted the wire transfer orders in good faith and in compliance with industry or commercial standards when it allowed 46 additional fraudulent wire transfers after the activity in Experi-Metal's account had been detected, after the customer had instructed Comerica that it should not honor any further wire transfers, and after Comerica's Treasury Management Department had instructed both the wire transfer room and the Electronic Data Management Department to stop all wire transfers and to terminate the session.

By: s/Richard B. Tomlinson
Richard B. Tomlinson (P27604)
DRIGGERS, SCHULTZ & HERBST, P.C.
Attorneys for Plaintiff
2600 West Big Beaver Road, Suite 550
Troy, MI 48084
Telephone: 248.649.6000
Facsimile: 248.649.6442
rtomlinson@driggersschultz.com

CERTIFICATE OF SERVICE

I hereby certify that on February 2, 2011, I electronically filed the foregoing papers with the Clerk of the Court using the ECF system, which will send notification of such filing to the following ECF participants: Todd A. Holleman (P57699), Lara Lenzotti Kapalla (P67667) and Boyd White, III (P72398).

Richard B. Tomlinson
2600 W. Big Beaver Rd., #550
Troy, Michigan 48084
Phone: (248) 649-6000
E-mail: cmacpherson@driggersschultz.com
P27604