UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

EXPERI-METAL, INC.,
a Michigan corporation,

Plaintiff,

Case No. 2:09-CV-14890

v.

Hon. Patrick J. Duggan

COMERICA, INC.,
a foreign corporation,

Defendant.

Richard B. Tomlinson (P27604)
Daniel R. Boynton (P30359)
Joseph W. Thomas (P33226)
DRIGGERS, SCHULTZ & HERBST, P.C.
Attorneys for Plaintiff
2600 West Big Beaver Road, Suite 550
Troy, MI 48084
(248) 649-6000
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
(313) 963-7420
holleman@millercanfield.com
kapalla@millercanfield.com

COMERICA INCORPORATED'S AMENDED MOTION FOR SUMMARY JUDGMENT

Defendant, Comerica Incorporated, by its undersigned attorneys and pursuant to Fed. R. Civ. P. 56, moves for entry of an Order dismissing Plaintiff Experi-Metal Inc's Complaint. As more fully set forth in the incorporated brief, Experi-Metal cannot blame its bank for its loss when the bank followed the security procedure Experi-Metal agreed to, and Experi-Metal itself caused the loss by disclosing its secure online banking login ID, PIN, password and account information to a criminal. Comerica is filing this amended motion to make a minor change to the statement of facts in its brief to correct some formatting issues in the original brief.

Counsel for Comerica Incorporated sought concurrence for the relief set forth in this motion from counsel for Experi-Metal, but concurrence was denied.

Respectfully submitted,

MILLER, CANFIELD, PADDOCK AND STONE, P.L.C.
Todd A. Holleman (P57699)
Lara Lenzotti Kapalla (P67667)

By: s/Todd A. Holleman
Attorneys for Defendant Comerica, Inc.
150 West Jefferson, Suite 2500
Detroit, MI 48226
(313) 963-6420
holleman@millercanfield.com

Dated: April 5, 2010

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

EXPERI-METAL, INC.,
a Michigan corporation,

Plaintiff,

Case No. 2:09-CV-14890

v.

Hon. Patrick J. Duggan

COMERICA, INC.,
a foreign corporation,

Defendant.

Richard B. Tomlinson (P27604)
Daniel R. Boynton (P30359)
Joseph W. Thomas (P33226)
DRIGGERS, SCHULTZ & HERBST, P.C.
Attorneys for Plaintiff
2600 West Big Beaver Road, Suite 550
Troy, MI 48084
(248) 649-6000
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
(313) 963-7420
holleman@millercanfield.com
kapalla@millercanfield.com

COMERICA'S AMENDED BRIEF SUPPORTING MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

ISSUES PRESENTED iii

CONTROLLING AUTHORITY iv

A. Regarding Motions For Summary Judgment iv

B. Regarding Customer Liability For Fraudulent Wire Transfers v

INTRODUCTION 1

STATEMENT OF FACTS 3

ARGUMENT 5

I. EXPERI-METAL'S COMPLAINT SHOULD BE DISMISSED BECAUSE IT CAUSED ITS OWN LOSS BY GIVING ITS SECURITY ID AND PASSWORD TO A CRIMINAL 5

A. The Security Procedure Used to Authenticate Experi-Metal's Transactions Was Commercially Reasonable 6

B. There Is No Genuine Dispute that Comerica Bank Followed the Security Procedure Experi-Metal Agreed to Use and Acted with Good Faith 8

C. Experi-Metal Admits It Was the Source of the Security Breach 10

CONCLUSION 11

INDEX OF AUTHORITIES

Page(s)

CASES

Anderson v. Liberty Lobby, 477 U.S. 242 iv

Audi AG v. D'Amato, 469 F.3d 534 (6th Cir. 2006) iv

Centre-Point Merchant Bank, Ltd v American Express Bank, Ltd, No. 95 Civ. 5000 LMM, 2000 WL 1772874 (S.D.N.Y. Nov. 30, 2000) 8, 9

Nix v. O'Malley, 160 F.3d 343 (6th Cir. 1998) iv

United States v. Miami University, 294 F.3d 797 (6th Cir. 2002) iv

Yamaha Motor Corp., U.S.A. v. Tri-City Motors and Sports, Inc., 171 Mich. App. 260, 429 N.W.2d 871 (1988 6

STATUTES

MICH. COMP. LAWS § 440.4605(1)(f) 9

MICH. COMP. LAWS § 440.4701 7

MICH. COMP. LAWS § 440.4702(2) ..... v, 6, 10

MICH. COMP. LAWS § 440.4702(3) 7, 8

MICH. COMP. LAWS § 440.4703 6

MICH. COMP. LAWS § 440.4703(1)(b) v

OTHER AUTHORITIES

U.C.C. § 4A-201, cmt 7

U.C.C. § 4A-203, cmt. 3 ..... v, 10

U.C.C. § 4A-203, cmt. 4 7

U.C.C. § 4A-203, cmt. 5 ..... v, 6

ISSUE PRESENTED

1. Can Experi-Metal recover against its bank when the bank followed the security procedures Experi-Metal agreed to and Experi-Metal itself caused the loss by giving its security ID, PIN, password and account information to a criminal?

   Comerica Incorporated answers: No

   Experi-Metal answers: Yes

CONTROLLING AUTHORITY

A. Regarding Motions For Summary Judgment

"A moving party is entitled to summary judgment as a matter of law 'if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact.' " *Audi AG v. D'Amato*, 469 F.3d 534, 542 (6th Cir. 2006) (quoting Fed. R. Civ. P. 56(c)). After the moving party makes this showing, the burden shifts to the nonmoving party to come forward with evidence demonstrating that there is a genuine issue of material fact for trial. *See id.*

To meet its burden, the non-moving party cannot rely on conclusory allegations, and must produce significant probative evidence that supports its pleadings. *See Nix v. O'Malley*, 160 F.3d 343, 347 (6th Cir. 1998); *Anderson v. Liberty Lobby*, 477 U.S. 242, 249-250; 106 S.Ct. 2505 (1986). In addition, "the mere existence of *some* alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment; the requirement is that there be no *genuine* issue of *material* fact." *Anderson*, 477 U.S. at 247-248 (emphasis in original). An issue of fact is genuine only if the evidence is such that a jury could return a verdict for the nonmoving party. *See id* at 248.

Summary judgment is appropriate before the close of discovery when, as here, discovery would not lead to genuine issues of material fact. *See United States v. Miami University*, 294 F.3d 797, 815-16 (6th Cir. 2002) (district court did not abuse discretion in denying discovery before granting summary judgment when discovery would not lead to genuine issues of material fact; district court was faced with issues of law, and purported need for discovery was irrelevant).

B. Regarding Customer Liability For Fraudulent Wire Transfers

The risk of loss is on the customer if a fraudulent payment order is accepted by the bank after verifying the authenticity of the source of the order in compliance with a commercially reasonable security procedure. *See* MICH. COMP. LAWS § 440.4702(2). The customer can avoid that risk only if it 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. *See* MICH. COMP. LAWS § 440.4703(1)(b); U.C.C. § 4A-203, cmt. 5. "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 the security procedure cannot be breached." U.C.C. § 4A-203, cmt. 3.

INTRODUCTION

This is a case that should never have been filed. It is undisputed that Experi-Metal gave its online banking login ID, PIN, password and account information to criminals in response to an internet "phishing" scam.[1] The criminals then used that information to access Experi-Metal's accounts at Comerica Bank and transfer money out of them. That resulted in Experi-Metal losing approximately $560,000. The applicable law and the parties' agreements establish, as a matter of law, that Experi-Metal is responsible for that loss and not Comerica Bank.

Experi-Metal wanted the convenience of internet banking. It asked Comerica Bank to provide this service, and agreed that the Bank would be using a system of login IDs, passwords, and a code that changed every 60 seconds ("RSA secure token technology") to verify, as Experi-Metal, the source of wire transfer payment orders. Experi-Metal agreed that the Bank's security procedure was commercially reasonable for Experi-Metal's use and wire transfer activity. It promised to keep its login and passwords confidential. The Bank offered Experi-Metal additional security protections, such as requiring more than one Experi-Metal user to log on to the system and approve any wire transfer, but Experi-Metal chose not to use those additional security protections.

Experi-Metal's account remained secure until January 22, 2009, when it broke its promise to safeguard its account login ID, PIN, password and account information. Comerica Bank had warned Experi-Metal of recent "phishing" attempts, whereby a third party

---

[1] Phishing is the "act of sending e-mail that purports to be from a reputable source, such as the recipient's bank or credit card provider, and that seeks to acquire personal or financial information. The name derives from the idea of 'fishing' for information." Encyclopedia Brittanica, http://www.britannica.com/EBchecked/topic/1017431/phishing

"In phishing, typically a fraudulent e-mail message is used to direct a potential victim to a World Wide Web site that mimics the appearance of a familiar bank or e-commerce site. The person is then asked to 'update' or 'confirm' their accounts, thereby unwittingly disclosing confidential information such as their Social Security number or a credit-card number." *Id.*

impersonating the Bank via email or the internet might ask for Experi-Metal's online ID and password information to "update" its systems. Comerica Bank specifically told Experi-Metal that it would *never* ask for a customer's ID or password information via email, and that Experi-Metal should not respond to any such requests purporting to come from Comerica Bank. Experi-Metal ignored that warning.

On January 22, 2009, Experi-Metal received a phishing email of the type Comerica Bank had warned it not to open, opened it, followed a link to a web page that asked for the security information Comerica Bank said it would never ask for, and entered its security information on the website. After Experi-Metal gave its online banking ID and password to the bogus website, the "phishers" used this information to access Experi-Metal's accounts and wire transfer over $1.9 million out of them.

Comerica Bank recovered some of the funds on behalf of Experi-Metal. Notwithstanding Comerica Bank's efforts on its behalf, Experi-Metal filed this suit and claimed that the online banking security procedures Comerica utilized were not commercially reasonable. Experi-Metal's claim fails because Comerica verified the source of payment orders pursuant to the agreed upon security procedures, which are deemed commercially reasonable as a matter of law when, as here, Experi-Metal was offered and declined additional security measures.

Comerica Bank's online security measures are like a lock, effective against anyone without a key. The criminal that accessed Experi-Metal's accounts was able to do so only because Experi-Metal gave him its key. That does not make the lock faulty, or render it unreasonable as a security device. In fact, in its contracts with Comerica, Experi-Metal agreed that Comerica's security procedures were commercially reasonable for its particular needs. Comerica followed those procedures. Experi-Metal did not. There was no problem until Experi-

Metal gave out its user ID, PIN, password and account information, contrary to its promise to safeguard them. Michigan law does not permit Experi-Metal to recover under these circumstances.

STATEMENT OF FACTS

In approximately 2000, Experi-Metal began banking with Comerica Bank. *See* Compl. ¶ 5. Experi-Metal wanted the convenience of remotely accessing its accounts using the internet so it entered online banking agreements with Comerica Bank. *See* Compl. ¶ 6. Experi-Metal agreed that the security procedures Comerica used were commercially reasonable for the type, size, and volume of transactions Experi-Metal would be conducting. *See* Ex 1, Comerica NetVision Wire Transfer agreement ¶ 3; Ex 2-B, Treasury Management Services Master Agreement p. 2 § 4.a. Experi-Metal also agreed that Comerica Bank could update and change its security procedures after giving notice to Experi-Metal. *See* Ex. 2-B at p. 2 § 4.c. Experi-Metal's continued use of the online banking system after such notice would constitute its acceptance of that new security procedure. *See id.*

In 2008, Comerica Bank gave Experi-Metal notice that the bank was going to implement an enhanced methodology to safeguard online accounts, utilizing RSA secure token technology. *See* Compl. ¶ 10. Under this system, users have to pass two tiers of security to initiate a wire transfer. At the first tier, the user logs on to the Comerica Business Connect website, which requires his or her user ID, 4-digit PIN, and the 6-digit code that is then displaying on his or her secure token. *See* Ex 2, Nosanchuk Affidavit ¶ 3. The randomly generated code displayed on the secure token changes every 60 seconds. *See id.* At the second tier, the user logs on to the Comerica Treasury Management Connect Web page, which requires his or her confidential customer ID, customer password, user ID, and user password. *See id* ¶ 4; Ex 2-A p. 1. Experi-Metal continued to access its accounts using this system, agreeing that the security system was

commercially reasonable. *See* Ex 2-B at p. 13 § 2.a. Experi-Metal also agreed that it would keep its passwords and IDs secure, and would be solely responsible for doing so. *See id* at § 2.

Comerica Bank offered additional security measures for customers when they made online wire transfers. Customer accounts could be set to require approval for wires from up to two other authorized users, or to require approval based on the dollar amount of the wires. *See* Ex 2 ¶¶ 7-10; Ex 2-A p. 18-19. Experi-Metal chose not to use or require these additional security procedures. *See* Ex 2 ¶ 12.

Comerica Bank became aware of a "phishing" scam, in which third persons were impersonating Comerica and other banks, and sending emails to their customers asking them to "register their Digital Certificate account by clicking on a link" that would then redirect them to a bogus internet site. *See* Ex 3, Cassa email.[2] On April 28, 2008, Comerica Bank sent an email to Experi-Metal and its other customers warning them about the fraudulent emails. *See id.* Comerica Bank gave Experi-Metal the following explicit warnings:

- DO NOT click any link within the email.
- Comerica has not issued an e-mail or any other communication requesting that a customer identify itself with a certificate or by any other means.
- Comerica is not adding digital certificate access to any of our online services.
- Comerica has no program to transition customers to a digital certificate that enables single sign-on access.
- Comerica will never initiate an unsolicited e-mail asking customers for their confidential information, such as IDs and passwords.

Id. This email reiterated warnings on Comerica Bank's website, in its user guides, *see* Ex. 1 at 32, and warnings and protections that have been well known to the public in general for years.

[2] Comerica Bank was using digital certificates as its method of verifying the authenticity of the source of a wire transfer payment order before it implemented its RSA secure token technology with two factor authentication. *See* Compl. ¶ 7.

See Ex. 4, October 2006 FTC Consumer Alert.

On January 22, 2009, Experi-Metal received one of these fraudulent emails. *See* Compl. ¶ 15. Ignoring Comerica Bank's warnings that it would "never" email users to ask for their security information and that customers should delete the emails without clicking on any links within them, the Experi-Metal user clicked on the link and gave Experi-Metal's ID, PIN and password to an unknown third party. *See* Compl. ¶¶ 16-18. After Experi-Metal gave the third party its security information, that party used that information to access Experi-Metal's accounts and place numerous wire transfer payment orders. *See* Compl. ¶ 18.

Following the security procedure Experi-Metal agreed to, Comerica authenticated the wire transfer payment orders with Experi-Metal user's ID, PIN and password. *See* Ex 2 ¶ 5; Ex 2-B p. 17 § 7.F. As Experi-Metal did not require confirmation of the transfers from a second or third Experi-Metal user, the Bank processed the wire transfers. *See* Ex 2 ¶ 12; Ex 5 ¶ 3. When Comerica Bank noted that a number of transfers had been made, it contacted Experi-Metal. *See* Compl ¶ 21. Contrary to its agreement with Comerica Bank, Experi-Metal asked the Bank not to honor any of the wire transfers, including those that had already been executed. *See* Compl ¶ 22; Ex 2-B p. 17 § 7.E. Comerica Bank put a hold on the account and tried to recover what funds it could. *See* Ex 6, Ling Affidavit ¶ 5; Ex 5 ¶¶ 4-6. Though Experi-Metal's credentials were used to authorize $1,901,269 in wire transfers, Comerica Bank was able to recover all but $560,000 for Experi-Metal. *See* Compl ¶ 24.

ARGUMENT

I. EXPERI-METAL'S COMPLAINT SHOULD BE DISMISSED BECAUSE IT CAUSED ITS OWN LOSS BY GIVING ITS SECURITY ID AND PASSWORD TO A CRIMINAL

When, as here, "an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure," "the

risk of loss [is] on the customer." U.C.C. § 4A-203, cmt. 5; *see also* MICH. COMP. LAWS § 440.4702(2).[3]

Experi-Metal can only avoid responsibility for the wire transfers if it can prove "that the person committing the fraud did not obtain the confidential information from an agent or former agent of the customer from a source controlled by the customer." U.C.C. § 4A-203, cmt. 5; *see also* MICH. COMP. LAWS § 440.4703. Here, Experi-Metal admits that the criminals got the user ID, PIN and password they used to access Experi-Metal's accounts from the Experi-Metal employee who entered them into the bogus website. *See* Complaint ¶¶ 16-18. In essence, Experi-Metal's employee gave the criminals the key to the lock which allowed them in. Experi-Metal cannot shift the blame for its loss to its bank when the lock operated properly.

A. The Security Procedure Used to Authenticate Experi-Metal's Transactions Was Commercially Reasonable

The security procedure Experi-Metal and Comerica Bank agreed to use to authenticate the source of wire transfer payment orders was commercially reasonable as a matter of law. *See* MICH. COMP. LAWS § 440.4702(3).[4]

> A security procedure is deemed 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,

[3] "Although the official comments do not have the force of law, they are useful aids to interpretation and construction of the UCC. Further, the comments were intended to promote uniformity in the interpretation of the UCC. Therefore, it is appropriate for this Court to consider the official comments when interpreting Michigan's UCC." *Prime Financial Services LLC v. Vinton*, 279 Mich. App. 245, 260 n.6; 761 N.W.2d 694 (2008); *see also Yamaha Motor Corp., U.S.A. v. Tri-City Motors and Sports, Inc.*, 171 Mich. App. 260, 270-71; 429 N.W.2d 871 (1988) (the Official Comments to the UCC are useful aids to interpret Michigan statutes adopting the UCC).

[4] The definition of "security procedure" limits the term to a procedure used to verify that a payment order is that of a customer "established by agreement of a customer and a receiving bank." MICH. COMP. LAWS § 440.4701; UCC § 4A-201, official cmt. It does not, as Plaintiffs urge, require an examination of all security measures in place at the Bank, but only those designated in the parties' agreements to verify the authenticity of a payment order received by the Bank.

> and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authenticated, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.

Id. "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." U.C.C. § 4A-203, cmt. 4.

Experi-Metal knew Comerica Bank was using RSA secure token technology and chose to continue using the online banking system. *See* Compl. ¶ 10. Experi-Metal agreed to use the RSA secure token technology offered by Comerica Bank and that the technology was commercially reasonable in light of the size, type, and frequency of payment orders it expected to make. *See* Ex 1; Ex 2-B p.2 §§ 4.a, c; p. 13 § 2.a. And, Experi-Metal agreed to be bound by payment orders issued in its name and accepted by the Bank in compliance with the agreed upon authentication procedure. *See* Ex 2-B p. 17 § 7.F.

Experi-Metal initiated only two wire transfers before January 22, 2009. *See* Complaint ¶ 14. Yet it was afforded the same protections as the Bank's high volume customers, *see* Ex 2 ¶ 11, making the agreed upon authentication process used by Comerica Bank even more reasonable under the circumstances. *See* U.C.C. § 4A-203, cmt. 4 (noting that high volume users may desire and reasonable expect "state-of-the-art" procedures that may be infeasible for lower volume users). Here, Comerica Bank offered and provided Experi-Metal with the same protections as similarly situated Bank customers, as well as more sophisticated Bank customers.

Although Experi-Metal could have required up to two other users to confirm every wire transfer payment orders its employee made, it chose not to require any such confirmations. *See* Ex 2 ¶ 12. Had Experi-Metal done so, the criminal that duped Experi-Metal's employee would not have been able to make authenticated payment orders that resulted in wire transfers unless he

had a second or third Experi-Metal employee also give him their security credentials. Thus, the security procedure Experi-Metal chose, after it was offered and refused additional protections, is deemed commercially reasonable. *See* MICH. COMP. LAWS § 440.4702(3); *see also* Ex 7, *Centre-Point Merchant Bank, Ltd v American Express Bank, Ltd*, No. 95 Civ. 5000 LMM, 2000 WL 1772874 at *5 (S.D.N.Y. Nov. 30, 2000) (security procedure under which plaintiff authorized bank to act on any telex messages that tested properly without further confirmation from plaintiff was commercially reasonable as a matter of law).

B. There Is No Genuine Dispute that Comerica Bank Followed the Security Procedure Experi-Metal Agreed to Use and Acted with Good Faith

Experi-Metal authorized Comerica Bank to process any online payment order authenticated with the security procedure described in the user guide. *See* Ex 2-B p. 16 § 7.A.1.6, p. 17 §7.C. The user guide provided that online wire transfers would be authenticated after Comerica received the user's ID, PIN, and RSA secure token code on Comerica Business Connect, followed by their customer ID and password and user ID and password on TM Connect Web. *See* Ex 2 ¶¶ 3-4; Ex 2-A p 1. Comerica followed this procedure. *See* Ex 5 ¶ 3. Though Experi-Metal alleges the Bank needed to call it to confirm online transfers, no such procedure is described in the user guide or in any agreement between the parties. *See* Ex 1; Ex 2-A; Ex 2-B.[5] Experi-Metal had the option of requiring internal confirmation of payment orders in any amount from a second or third Experi-Metal user, but it never exercised that option. *See* Ex 2 ¶ 12.

Comerica followed its agreements with Experi-Metal when it processed the wire transfers in question. Those agreements allowed wire transfers that would cause a zero or negative

[5] While phone confirmation was available for payment orders initiated by telephone, Experi-Metal opted for a security procedure "with no call back." *See* Ex 8, 12-1-07 Wire Transfer Authorization. As with the online payment orders, Experi-Metal agreed that if the party initiating the transfer presented correct identifying credentials (in that case, driver's license number and mother's maiden name) no further confirmation was required.

balance in Experi-Metal's accounts. Experi-Metal authorized Comerica to "debit the Authorized Account for any payment Order and applicable fees, even if the debit creates or increases an overdraft position or line of credit in the Authorized Account." Ex 2-B p. 17 § 7.J. *See also id* at p.3 § 11 (authorizing Bank to process withdrawals and transfers when there are insufficient funds); p. 16 § 7.A.1.2 (stating that if there are insufficient funds in an account, "the Bank may debit or draw on any account(s) Customer has with the Bank and such account(s) will be an Authorized Account" for executing a payment order). There is no genuine issue of fact that Comerica Bank followed the procedure Experi-Metal agreed to. *See* Ex 7, *Centre-Point Merchant Bank, Ltd*, 2000 WL 1772874 at * 5 (finding bank followed the agreed upon security procedure when no evidence supported customer's allegation that bank was supposed to verify telex instructions by phone).

There is also no genuine issue of fact that Comerica Bank accepted the payment orders submitted with Experi-Metal's credentials in good faith. "'Good faith' means honesty in fact and the observance of reasonable commercial standards of fair dealing." MICH. COMP. LAWS § 440.4605(1)(f). Here, Comerica Bank accepted and processed the payment orders submitted using Experi-Metal's online credentials as the parties had agreed Comerica Bank would do. Experi-Metal makes the conclusory allegation that this was not done by Comerica Bank in good faith, but it fails to allege any factual support for its claim. *See* Compl. ¶ 29. Comerica Bank complied with its agreements with Experi-Metal and, thus, acted honestly and dealt fairly with Experi-Metal. There is no allegation or evidence that can be made or presented to the contrary.

Moreover, Comerica Bank was the party that alerted Experi-Metal to a potential problem. *See* Compl ¶ 21; Ex 6. The parties did not by their agreement impose any duty on Comerica Bank to monitor Experi-Metal's account for increased wire transfer activity or to call Experi-

Metal to verify authenticated wire transfer payment orders. *See* Ex 1; Ex 2-A; Ex 2-B. But Comerica Bank did this anyway. *See* Ex 5 ¶¶ 3-4. When Experi-Metal asked Comerica Bank not to honor any of the transfers, including those that had already been executed, it was again asking the Bank to go beyond the parties' agreements. *See* Ex 2-B p. 17 § 7.E (stating that the bank has no obligation to stop payment of any transfers and that those already executed "cannot be canceled, amended, or stopped."). MICH. COMP. LAWS § 440.4702(2) recognizes that the bank is "not required to follow an instruction that violates a written agreement with the customer." Comerica Bank went above and beyond its contractual and statutory duties to help Experi-Metal undo the damage Experi-Metal itself had caused. *See* Ex 6 ¶¶ 4-5; Ex 5 ¶¶ 4-6. Though Experi-Metal's credentials were used to authorize $1,901,269 in wire transfers, Comerica Bank was able to recover all but approximately $560,000 for Experi-Metal. *See* Compl ¶ 24.

C. Experi-Metal Admits It Was the Source of the Security Breach

Experi-Metal knew that it was responsible for keeping its user passwords and IDs confidential. *See* Ex 1 ¶ 3; Ex 2-B p. 13 § 2, 2.a. It knew it was supposed to delete emails "asking customers for their confidential information, such as IDs and passwords." *See* Ex 3. But it did not do so.

Experi-Metal admits that a criminal got its User ID, PIN and password because one of its employees followed a link in a phishing email and provided this information to a bogus website. *See* Complaint ¶¶ 16-18. Experi-Metal was responsible for this security breach. *See* U.C.C. § 4A-203, cmt. 3 ("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 the security procedure cannot be breached.") Consistent with Michigan law and common sense, Experi-Metal cannot shift responsibility for its resulting loss to

Comerica.

CONCLUSION

For the foregoing reasons, Comerica Incorporated respectfully requests this Court to dismiss Experi-Metal, Incorporated's Complaint against it.

Respectfully submitted,

MILLER, CANFIELD, PADDOCK AND STONE, P.L.C.
Todd A. Holleman (P57699)
Lara Lenzotti Kapalla (P67667)

By: s/Todd A. Holleman
Attorneys for Defendant Comerica, Inc.
150 West Jefferson, Suite 2500
Detroit, MI 48226
(313) 963-6420
holleman@millercanfield.com

Dated: April 5, 2010

CERTIFICATE OF SERVICE

I hereby certify that on April 5, 2010, I electronically filed the foregoing paper with the Clerk of the Court using the ECF system and the Court will send notification of such filing to the parties.

Richard B. Tomlinson - rtomlinson@driggersschultz.com

s/Todd A. Holleman
Miller, Canfield, Paddock and Stone, PLC
150 West Jefferson, Suite 2500
Detroit, MI 48226
(313) 963-6420
holleman@millercanfield.com