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

EXPERI-METAL INC.,
a Michigan corporation,

Plaintiff,

Case No. 2:09-cv-14890

vs.

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

---

# EXPERI-METAL, INC.'S RESPONSE TO COMERICA BANK'S AMENDED MOTION FOR SUMMARY JUDGMENT

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

## COUNTER-STATEMENT OF ISSUES PRESENTED

1. Can Comerica Bank avoid liability for paying on a payment order or wire transfer which was not initiated by Experi-Metal, not authorized by Experi-Metal, and not initiated by an agent of Experi-Metal?

   Comerica Bank answers: Yes

   Experi-Metal answers: No

2. Can Comerica Bank avoid liability for such wire transfers where the Bank and Experi-Metal never agreed to the security procedures instituted by Comerica Bank?

   Comerica Bank answers: Yes

   Experi-Metal answers: No

3. Can Comerica Bank avoid liability for such transfers where the security procedures used by Comerica Bank were not a commercially reasonable method of providing security against unauthorized payment orders and where the Bank has not shown that it accepted the payment orders in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer?

   Comerica Bank answers: Yes

   Experi-Metal answers: No

## INTRODUCTION

This is a motion that should have never have been filed.

In May, 2008, Comerica instituted a change in its on-line wire transfer service for Experi-Metal. Comerica had previously offered NetVision Wire Transfer Service and in connection with that service, had used a security process known as "digital certificates" for verifying that it was Experi-Metal that was wire transferring funds from Experi-Metal's accounts at Comerica. Experi-Metal signed an agreement with Comerica setting forth the terms for the NetVision Wire Transfer Services, which was attached to Defendant's Motion as Exhibit 1.

In late April, 2008, Comerica advised Experi-Metal that the wire transfer service available for Experi-Metal would be through TM Connect Web ("TMC Web") and would no longer be through NetVision Wire Transfer. At the same time Comerica advised Experi-Metal that the security process would also change, "digital certificates" would no longer be used, and that a "secure token" security process would be used in connection with the new service. At the time that Comerica instituted the change, Experi-Metal was not given any other options or alternatives to the secure token technology and in fact, never even signed an agreement for the new TMC Web wire transfer service (Allison Affidavit which is attached as Exhibit 1). Experi-Metal never entered into any agreement for TMC Web wire transfer services and never agreed that the "secure token" technology was "commercially reasonable." Likewise, after Comerica initiated TMC Web wire transfer service, Experi-Metal never made any wire transfers using the service. At the time the TMC Web wire transfer service and secure token technology was instituted by Comerica, Experi-Metal was not advised that the Experi-Metal account could be set up to require approval from one or more persons for each wire transfer or each wire transfer based on dollar amount, nor was Experi-Metal advised of any additional security features that

could be used to protect Experi-Metal with respect to the TMC Web wire transfer service. (Ex. 1)

In summary, Experi-Metal never entered into a written agreement with Comerica for the TMC Web wire transfer service, never agreed to the use of the secure token technology to verify Experi-Metal as the source of wire transfer payment orders, never agreed that the bank's security procedure was commercially reasonable for Experi-Metal's wire transfer activity, was never offered additional security provisions under the TMC Web wire transfer service and never initiated any wire transfers. As a result, Comerica's Motion must be denied and Plaintiff should be awarded its reasonable attorneys' fees incurred in responding to this baseless motion.

## I. STATEMENT OF FACTS

As noted in the Affidavit of Valiena Allison, President and CEO of Experi-Metal, Experi-Metal began banking with Comerica Bank in approximately September, 2000 (Ex. 1, ¶3). Experi-Metal did not ask Comerica Bank to provide internet banking services. Sales and marketing representatives from Comerica approached Experi-Metal, and convinced Experi-Metal of the advantages of internet banking. Comerica's representative's touted Comerica's expertise in providing excellent security in connection with their on line banking system (Ex. 1, ¶4). At all times Experi-Metal followed Comerica's advice with respect to security processes as Experi-Metal believed Comerica's statements regarding their expertise and security and followed Comerica's lead (Ex. 1, ¶4).

From approximately 2001 through approximately May, 2008, Comerica offered on-line banking and wire transfer service to Experi-Metal through a service called NetVision Wire Transfer Services (Ex. 1, ¶5). In fact, Experi-Metal signed a written agreement with Comerica agreeing to the NetVision Wire Transfer Services (Ex. 1, ¶5). From approximately 2001 through May, 2008, Comerica used a security process known as "digital certificates" as security for

Comerica's NetVision Wire Transfer Service, to prevent unauthorized access to and withdrawals from customer accounts (Ex. 1, ¶6). Under that system the digital certificate was loaded on a particular computer at Experi-Metal and access to NetVision could only be had from a computer that had a digital certificate loaded on that computer (See Lance James Declaration, attached as Exhibit 2). Periodically, Experi-Metal was required to designate to Comerica the individuals within the company who were authorized to initiate a wire transfer from the Company's accounts (Exhibit 3).

In late April of 2008, Comerica advised Experi-Metal that beginning in May, 2008, on-line wire transfer services would be through a system called TMC Web rather than NetVision Wire Transfer Services (Ex. 1, ¶8). At the same time, Comerica advised Experi-Metal that the security technology was being changed to a "secure token" methodology for access to TMC Web and the wire transfer services (Ex. 1, ¶9). On April 25, 2008, Comerica provided Experi-Metal with the secure tokens and IDs to be used to connect to TMC Web and its letter indicated that the secure token system would go into effect in May, 2008 (Ex. 1, ¶11).

At the time that the change to the TMC Web for wire transfer service and the secure token technology were instituted by Comerica, Experi-Metal was not given any other options or alternatives to the secure token technology (Ex. 1, ¶12). In addition, Experi-Metal never even signed a written agreement for the new TMC Web wire transfer service (Ex. 1, ¶12). At the time of the change to the secure token technology, Experi-Metal was not advised that Experi-Metal's accounts could be set up to require approval of more than one person for each wire transfer, or each wire transfer based on a dollar amount, nor was Experi-Metal advised of any additional security features that could be used to protect Experi-Metal with respect to wire transfers or on-line banking (Ex. 1, ¶13). In addition, Valiena Allison did not receive training on the use of Comerica's wire transfer service through the TMC Web at the time the change was made to the

secure token technology (Ex. 1, ¶14). In fact, at no time did Comerica offer any additional security procedures to Experi-Metal with respect to wire transfers through the TMC Web (Ex. 1, ¶15).

Experi-Metal never agreed that the security procedures utilized by the TMC Web wire transfer service were commercially reasonable, and after Comerica instituted the wire transfer service through TMC Web, Experi-Metal never even used the wire transfer service after it was implemented by Comerica (Ex. 1, ¶¶16, 18).

From 2001 through April 29, 2008, while Experi-Metal was using the NetVision Wire Transfer Services, Comerica regularly sent emails to Experi-Metal with respect to the renewal of Experi-Metal's digital certificates (Maslowski Affidavit, attached as Exhibit 4, ¶3). The emails, copies of which are attached as Exhibit 5, required Experi-Metal to click on a link specified in the email. Once linked on the web site, Experi-Metal was required to log in and enter Experi-Metal's confidential customer ID number and customer banking information in order to obtain the renewal of Experi-Metal's digital certificate (Ex. 4, ¶3).

On January 22, 2009, Keith Maslowski, Experi-Metal's Controller, received an email that appeared to be from Comerica and was similar to the emails that Experi-Metal had received from 2000 through 2008 from Comerica (Ex. 4, ¶4). The email, like the prior emails from Comerica, required Experi-Metal to click on a link specified in the email which appeared to be a Comerica website (Ex. 4, ¶5). Once linked on the "Comerica" website, Maslowski was required to log in and enter Experi-Metal's and his confidential customer ID number and confidential banking information as it had in the past (Ex. 4, ¶6). Interestingly, Maslowski has never been designated by Experi-Metal as someone who was authorized to initiate wire transfers from the Company's sweep account (Ex. 1, ¶17). After providing that information, unknown and unauthorized third parties obtained the information, logged into Comerica's online banking site, and began using

the TMC Web wire transfer service to initiate wire transfers out of Experi-Metal's sweep bank account, sending the funds to various accounts in Russia, Estonia, Scotland, Finland and China, as well as domestic accounts (Ex. 4, ¶7). In fact, between 7:30 a.m. and 10:50 a.m., 47 unauthorized and fraudulent wire transfers were made from Experi-Metal's bank accounts (Ex. 4, ¶8).

Despite all of the wire transfers and unusual activities in Experi-Metal's accounts, Comerica did not contact Experi-Metal until 10:50 a.m., when a representative of Comerica finally called Experi-Metal, and asked whether Experi-Metal was aware of any of the outgoing wire transfers (Ex. 1, ¶20). Experi-Metal immediately instructed Comerica that Experi-Metal had not made any wire transfers and Comerica was not to honor any requested wire transfers until further notice (Ex. 1, ¶21). In spite of this direct instruction, Comerica failed to abide by Experi-Metal's request, and from 10:53 a.m. until 2:02 p.m., there were an additional 41 fraudulent wire transfers made from Experi-Metal's bank accounts (Ex. 4, ¶9). As a result, Experi-Metal's accounts were charged approximately $560,000 for unauthorized wire transfers. Experi-Metal has filed this action to recover its losses.

## II. ARGUMENT

### A. Standard of Review

Defendant has moved for summary judgment pursuant to Rule 56C of the Federal Rules of Civil Procedure. Under Rule 56C, summary judgment may be granted only if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show there is no genuine issue as to any material fact, and that the moving party is entitled to judgment as a matter of law. The Court must view the evidence in the light most favorable to the nonmoving party and draw all reasonable inferences in the nonmoving party's favor. *United States v Diebold, Inc.*, 369 US 654 (1962).

**B. Article 4A of the Uniform Commercial Code**

Article 4A of the Uniform Commercial Code (UCC) governs the allocation of fraud losses arising from funds transfers for business accounts. Article 4A of the UCC has been enacted in Michigan, MCLA 440.4601 *et seq.*

The relevant provisions for allocating fraud losses arising from funds transfers for business accounts start with MCLA 440.4701 where the term "security procedure" is defined as follows:

> "'Security procedure' means a procedure established by agreement of a customer and a receiving bank for the purpose of
>
> (i) Verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or
> (ii) Detecting error in the transmission of the content of the payment order or communication."
>
> . . .

MCLA 440.4702(2) provides the factors to be examined by the court with respect to analyzing the security procedures at issue in such a case as follows:

MCLA 440.4702(2), (UCC Section 4A-202(b)) specifies:

> "If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender, will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if
>
> (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and
>
> (ii) The bank proves that it accepted the payment order in good faith and in compliance with the security procedure in any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer."

Under these sections, fraud losses may fall on the business customer only if:

(1) the business and the bank have agreed to the use of the security procedures at issue to verify the authenticity of payment orders;

(2) the security measures that have been agreed upon by the bank and the customer are commercially reasonable;

(3) the bank has in fact employed those security procedures with respect to the transfers being analyzed; and

(4) the bank has acted in good faith and in compliance with any written instructions of the customer restricting acceptance of payment orders initiated in the customer's name.

The facts and circumstances in this case demonstrate a genuine issue of material fact with respect to each of the factors.

**C. There are genuine issues of material fact as to whether Comerica Bank and Experi-Metal agreed to the security procedures at issue in this case.**

Defendant argues as an undisputed fact, that Defendant and Experi-Metal entered into a written agreement, agreeing that the security procedures used by the Defendant in this case were commercially reasonable for the type, size and volume of the transactions that Experi-Metal would be conducting. Interestingly, the agreement cited by Comerica in support of this argument is Experi-Metal's previous written agreement with Comerica for the NetVision Wire Transfer Services, which was executed in November of 2003. As noted by the Affidavit of Valiena Allison, when Defendant changed and instituted the TMC Web wire transfer service in May of 2008, Experi-Metal never signed any agreement for the TMC Web wire transfer service (Ex. 1, ¶12). In the absence of a written agreement for the TMC Web wire transfer service, there was no agreement between the bank and its customer as to the security procedure to be used to test the authenticity of payment order as is required under MCLA 440.4701 for the application of MCLA 440.4702(2). Likewise, there was certainly no agreement by Experi-Metal that the security procedure instituted by Defendant in connection with the TMC Web wire transfer service was

commercially reasonable as argued by Defendant. The NetVision Wire Transfer Services agreement relied upon by Defendant in support of its argument, has no application to the TMC Web wire transfer service instituted in May of 2008, has no application to the wire transfers or security procedures that were in place on January 22, 2009, and is irrelevant to this dispute.

Comerica also argues that under the terms of the 2002 Treasury Management Services Master Agreement, Defendant and Experi-Metal agreed to Defendant's security measures as to the authenticity of payment orders. The problem with Defendant's argument in this regard, is that Experi-Metal was not a signatory to the Treasury Management Services Master Agreement attached to Defendant's motion and brief. More importantly, by its terms, the Treasury Management Services Master Agreement has no application to the TMC Web wire transfer service at issue in this case. By its terms, the Treasury Management Services Master Agreement indicates at page 1:

> "This Agreement governs the customer and Comerica, Incorporated subsidiary bank(s) "bank" as to each Service for which they have executed a Service Agreement." (emphasis added)

As noted above, Experi-Metal never signed an agreement for the TMC Web wire transfer service (Allison Affidavit, ¶12). As a result, there was no executed service agreement for wire transfer services and therefore, by its terms, the Treasury Management Services Master Agreement has no application in this case. As a result, Defendant and Experi-Metal never "agreed" as to the security procedures to be used to verify a payment order under MCLA 440.4701 and 440.4702(2).

Defendant has also attempted to argue that Experi-Metal's continued use of the wire transfer service after notice of the Bank's change in security procedure constituted Experi-Metal's acceptance of the new security procedure for wire transfers. However, as noted by the Affidavit of Valiena Allison, after Comerica implemented the TMC Web wire transfer service in

May of 2008, and implemented the "secure token" technology in May, 2008, Experi-Metal never sent even a single wire transfer (Ex. 1, ¶18). Since Experi-Metal never used the TMC Web wire transfer service, there was no continued use of the service, and therefore, no acceptance of the security procedure to be used to verify payment orders under MCLA 440.4701 and 440.4702(2).

Defendant has also attempted to argue that the "Treasury Management Connect Web User Guide" which was attached as Exhibit 2A to Defendant's Motion, somehow constituted an agreement between the Defendant and Experi-Metal as to the security procedure to be used to verify a payment order under the TMC Web wire transfer service. However, the User Guide relied upon by Defendant in support of its Motion and in some of the affidavits submitted by Defendant was never even provided to Experi-Metal (Ex. 1, ¶11).

In the absence of a commercially reasonable security procedure being agreed to by the parties, MCLA 440.4702(2) (UCC Section 4A-202(b)) does not apply and Official Comment 1 to the Uniform Commercial Code provides that in the absence of a commercially reasonable security procedure:

> "The result is that subsection (a), [MCLA 440.4702(1)] applies and the bank acts at its peril in accepting a payment order that may be unauthorized."

MCLA 440.4702(1) (UCC Section 4A-202(a)) provides:

> "A payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order, or is otherwise bound by under the law of agency."

The facts in this case and the Affidavits demonstrate that Experi-Metal did not initiate the wire transfers at issue in this case, and that the initiator of the wire transfers was not authorized by Experi-Metal to initiate the transfers and was not an agent of Experi-Metal. Under MCLA 440.4702(1) and the Official Comment, the bank acted at its peril in accepting the payment orders.

**D. There are genuine issues of material fact as to whether Defendant's security procedure was commercially reasonable.**

If the Court concludes that MCLA 440.4702(2) applies with respect to the issues in this case, rather than MCLA 440.4702(1), summary judgment is not warranted because there are genuine issues of material fact as to whether the "secure token" security procedure that was implemented by Defendant in May, 2008, to verify wire transfers under the TMC Web wire transfer service was commercially reasonable under MCLA 440.4702(2)(i).

**1. MCLA 440.4702(3) does not apply to the facts of this case.**

Defendant has argued that the security procedure used by Defendant, secure token technology, was commercially reasonable as a matter of law under MCLA 440.4702(3) which provides in relevant part:

> "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; 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."

Comerica's security procedure does not meet the requirements of MCLA 440.4702(3) and therefore is not deemed commercially reasonable as a matter of law. First, the secure token technology procedure that was instituted by Comerica in May of 2008 was not a procedure that was selected by the customer after the bank offered and the customer refused a security procedure that was commercially reasonable for that customer. Defendant has relied on the Affidavit of Deborah S. Nosanchuk in support of its claim that Defendant offered Experi-Metal additional security procedures and those procedures were refused, or not selected, by Experi-

Metal. The Affidavit of Valiena Allison, directly contradicts Ms. Nosanchuk's Affidavit and clearly states that at the time the TMC Web wire transfer service was initiated by Comerica, Experi-Metal was never advised that the Experi-Metal account could be set up to require approval for more than one person for each wire transfer, or each wire transfer based on a certain dollar amount, nor was she advised of any additional security features that could be used to protect Experi-Metal with respect to wire transfers or on line banking (Ex. 1, ¶ 13). In fact, Allison's Affidavit expressly notes that Comerica did not offer any additional security procedure in connection with the TMC Web wire transfer service and that Experi-Metal was not given any other alternative (Ex. 1, ¶¶ 12, 14 and 15). Accordingly, there are genuine issues of fact as to whether Defendant ever offered alternative security measures, and whether Experi-Metal refused those security procedures, which is the first element required by MCLA 440.4702(3).

In addition, the second element of MCLA 440.4702(3) is not met in this case as Experi-Metal never expressly agreed in writing to be bound by a payment order issued in its name and accepted by the Bank in compliance with the security procedure chosen by the customer. In fact, the Affidavit of Valiena Allison demonstrates that Experi-Metal never entered into a written agreement agreeing to the TMC Web wire transfer service and the related security procedure (Ex. 1, ¶12). In addition, Experi-Metal never initiated a wire transfer or used the TMC Web wire transfer service after it was instituted by Comerica (Allison Affidavit, ¶18).

Accordingly, neither of the elements of MCLA 440.4702(3) is satisfied in this case and therefore Defendant's security procedure is not deemed to be commercially reasonable under the statute as a matter of law.

**2. Defendant's security procedure was not commercially reasonable.**

What constitutes a commercially reasonable security procedure is determined in light of the wishes of the bank's customer that are expressed to the bank, the circumstances of the

customer known to the bank (including the size, type and frequency of payment orders normally issued by the customer to the bank), alternative security procedures offered by the bank to the customer, and security procedures in general use by customers and their banks. (UCC, Section 4A-203, Comment 4 (MCLA 440.4703, Comment 4)).

As noted above, Defendant's security procedure fails with respect to each of these factors. In May of 2008, Defendant simply imposed the "secure token" technology with no discussion with the customer to determine the needs of the customer, and failed to offer the customer alternative or additional security procedures to protect the customer's accounts.

As noted in the Declaration of Lance James, Plaintiff's expert witness in this case, the secure token technology that was implemented by Comerica in May of 2008, was not a commercially reasonable security procedure for a number of reasons. First, as noted by James, the secure token technology was known at that time to be lacking in any reasonable defense to a man-in-the-middle phishing attack such as what occurred in this case, and has generally been unacceptable for login security purposes in the banking community since approximately 2003. As noted by James, Defendant's implementation of the secure token technology in May of 2008 was particularly dangerous based on the background of the relationship between Defendant and Experi-Metal. As noted in the Affidavit of Keith Maslowski, from 2001 through 2008, while Experi-Metal was using the NetVision Wire Transfer Service, Defendant regularly sent unsolicited emails to Experi-Metal. Those emails required Experi-Metal to click on a link specified in the email. Once linked in to the website, Experi-Metal was required to login and enter Experi-Metal's confidential customer ID number, password numbers and other confidential information in order to obtain the renewal of Experi-Metal's digital certificates under that system. As a result, Defendant had "trained" Experi-Metal, to receive unsolicited emails from Comerica, link onto a website, and voluntarily provide customer ID number, password, and other

confidential information as part of its online banking activities (Ex. 2). The "training" provided by Comerica over the preceding seven years made Experi-Metal extremely vulnerable to the man-in-the-middle phishing attack which occurred in this case. Experi-Metal had become accustomed to receiving unsolicited emails from Comerica requiring Experi-Metal to link onto a website and provide its confidential online banking information (Ex. 2). Defendant's Amended Motion and Brief make it clear that at the time of Defendant's conversion to the "secure token" technology, Comerica was well aware of the danger of "phishing scams" in which a third party would impersonate Comerica to send emails to the customer and ask them to click on a link and provide confidential banking information (Defendant's Brief, p. 4). Comerica's switch to the secure token technology under these circumstances was certainly not commercially reasonable, and certainly put Comerica's customers at risk, especially in light of the "e-mail history" between Defendant and its customers (Ex. 2).

Defendant's Brief in support of its Amended Motion attempts to blame Experi-Metal for the losses in this case, because Experi-Metal provided the criminal with its confidential information by entering that information into a bogus website. In fact, Comerica characterizes Experi-Metal's actions as having given the criminals "the key to the lock" which allowed them into Experi-Metal's account. Defendant attempts to laud its security procedures by pointing out that on April 28, 2008, Defendant sent an email to its customers warning them about potential for fraudulent emails and man-in-the-middle phishing attacks, and attaches a copy of the "warning" email as Exhibit 3 to Defendant's Amended Motion. In the "warning" email, Defendant warned stating "Comerica will never initiate an unsolicited e-mail asking customers for their confidential information, such as IDs and passwords." Defendant then argues that Experi-Metal then ignored Defendant's warning that it would never ask for confidential security information in an unsolicited email. The fact of the matter is that on April 29, 2008, exactly one day after

Comerica sent out its "warning" email, Comerica violated its own policy, sent an unsolicited email to Experi-Metal, requiring Experi-Metal to click on the link specified in the email, and login with its confidential information into the site (Exhibit 6 attached hereto and Maslowski Affidavit). Under these circumstances, Comerica created confusion, conflict and uncertainty for its customers and misrepresented its own policy in the "warning" e-mail.

Defendant's actions in converting to "secure token" technology in light of the prior "e-mail history" with its customers, was not commercially reasonable (Ex. 2). Comerica's failure to provide Experi-Metal with security alternatives or to alert the customer to other security alternatives, such as requiring up to two users to confirm every wire transfer payment was also commercially unreasonable (Ex. 2).

This case is clearly distinguishable from *CentrePoint Bank, Ltd. v American Express Bank, Ltd.,* No. 95 Civ 5000 LMN 2000 WL 1772874 (SD, NY November 30, 2000) relied upon by Defendant. In that case, the security procedure which the plaintiff customer chose was selected after Plaintiff was offered and refused additional protections. In this case, Experi-Metal was not offered additional security protection, nor advised of the existence of alternate security measures (Ex. 1).

**3. The Secure Token technology was not commercially reasonable and failed to provide and maintain authentication of verification.**

Defendant's secure token technology is a security process that only provides login authentication and provides no protection in terms of transaction verification or verifying the wire transfers initiated after the initial login. As described in the Affidavit of Debra S. Nosanchuk, which was attached as Exhibit 2 to Defendant's Amended Motion, the secure token technology operates with the following steps:

> "To access this website, the user must log on by entering his or her user ID, his or her confidential 4-digit PIN, and a six-digit code from a secure token…" (Nosanchuk Affidavit, ¶3)
>
> "In order to make wire transfers, the user must log onto the TMC Web…by first entering their confidential customer ID and customer password, and then entering the individual user's confidential user ID and user password." (Nosanchuk Affidavit, ¶4)

Although Defendant touts the six-digit code from the secure token, and the fact that the secure token is a randomly generated number that changes every sixty seconds, the Defendant's security system only requires a user to enter the six-digit code from a secure token in the first step to log into the website. Once in the website, the user is able to access the TMC wire transfer service in order to initiate online wire transfers without entering the six-digit code from the secure token for again. Likewise, once the user is into the TMC Web wire transfer service, the user is able to sit at a computer and initiate individual wire transfers from the account, transaction after transaction, without ever having to use the sig-digit code from the secure token to initiate any of the wire transfers. As a result, once a criminal gets into the system with the initial misappropriation of the IDs and passwords, the criminal is able to generate as many wire transfers as he/she wants, without ever having to use the six-digit from the secure token again.

Defendant's Brief and Affidavits tout the fact that the six-digit from the secure token is a randomly generated number that changes every sixty seconds. Defendant fails to point out that its security system only requires the use of the six-digit code at the first step in order to log in, and does not require repeated use of the code for subsequent transaction verification. As a result, the fact that the code is randomly generated and changes every sixty seconds provides absolutely no security except for log in authentication as the security procedure does not require any transaction verification by repeated use of the ever changing code (Ex. 2). In this case, once the criminal misappropriated the information, he was able to immediately sit down and generate 93

wire transfer transactions from Experi-Metal's accounts without ever having to re-enter the ever changing six-digit code from the secure token, other than the initial log in. This renders Defendant's security system commercially unreasonable as it provided no additional verification for the 93 wire transfer transactions which were completed after the initial log in authentication (Ex. 2). Had the criminal been forced by Comerica's security system to authenticate or verify each transaction by putting in the ever changing six-digit code from the secure token, the criminal would have been stopped before the first wire transfer had been sent since the criminal did not have access to the continually changing six-digit code after the first sixty seconds. Clearly, Defendant's security system requiring only login authentication is not a commercially reasonable method of providing security against unauthorized payment orders/wire transfers.

The official Comment 4 to Section 4A-203 of Article 4A of the UCC (MCLA 440.4703) discusses the factors to be examined in determining what constitutes a commercially reasonable security procedure. Comment 4 specifically notes that the type of payment order is a variable to be considered in determining the commercial reasonableness of the security system, noting in part:

> "The type of payment order is another variable. For example, in a wholesale wire transfer, each payment order is normally transmitted electronically and individually. A testing procedure will be individually applied to each payment order." (Emphasis added)

Obviously, the secure token system that was instituted by Comerica provided only login authentication or verification using the six-digit code from a secure token. Defendant's security system did not require the ever changing six-digit code to be utilized to verify each of the payment orders or transactions, thereby foregoing a testing procedure for each payment order as required in the Comment.

**E. There are genuine issues of material fact as to whether the Bank has proven that it accepted the payment orders in good faith and in compliance with the security procedures.**

Under MCLA 440.4702, Defendant is required to prove that it accepted the payment orders in good faith and in compliance with the security procedures and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. Defendant has failed to make that showing.

Good faith is defined in MCLA 440.4605 as "honesty in fact and the observance of reasonable commercial standards of fair dealing." Plaintiff submits that reasonable commercial standards of fair dealing would not entail allowing 47 fraudulent wire transfers to be initiated from Plaintiff's bank account, particularly with respect to a customer which had made only two wire transfers in the prior two years, with those transfers being made in 2007. Likewise, reasonable commercial standards of fair dealing would not include allowing an additional 46 fraudulent wire transfers to be initiated after being instructed by the Plaintiff that Plaintiff had initiated any wire transfers, and had instructed Defendant not to honor any further transfers. As noted in the Declaration of Lance James, a simple fraud scoring system or fraud monitoring program to monitor the accounts for unusual activity, such as those routinely used by credit card companies on a daily basis, would have stopped the fraud very quickly and been within reasonable commercial standards of good faith and fair dealing. Likewise, sending those unusual wire transfers to unusual destinations such as Moscow, Estonia and China, likewise do not demonstrate good faith, particularly in light of Plaintiff's limited prior use of wire transfers. As noted in the prior section, the security procedure imposed by the Defendant did not require the user to enter the ever changing secure token code except at the time of the initial login. The failure to require repeated use of the secure token for each of the payment orders or wire transfer transactions, also reflects a lack of good faith and commercial reasonableness.

Likewise, Defendant has not shown that it acted in compliance with the "security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer." As noted above, there simply was no written agreement between the parties as to the TMC Web wire transfer service or the security procedure to be used in connection with the wire transfer service and therefore, there could be no compliance with the "security procedure" as that term is defined in MCLA 440.4701. In addition, Keith Maslowski was never authorized by Experi-Metal as an individual with authority to initiate wire transfer orders on behalf of Experi-Metal from the account from which the wire transfers were made in this case (Ex. 1, ¶17). From time to time, Experi-Metal gave the Defendant written notification of those persons authorized by Experi-Metal to initiate wire transfer orders with respect to the various accounts, and it did not include Mr. Maslowski (Ex. 3).

Furthermore, on January 22, 2009, when the customer did give specific verbal instructions that no wire transfers were to be honored, Defendant did not adhere to that instruction and 46 additional wire transfers were allowed.

## CONCLUSION

For the foregoing reasons, Experi-Metal requests this Court to deny Defendant's Motion and award Experi-Metal its attorneys' fees incurred in having to respond to this motion.

Respectfully submitted,

DRIGGERS, SCHULTZ & HERBST, P.C.

By: s/Richard B. Tomlinson
Richard B. Tomlinson (P27604)
Daniel R. Boynton (P30359)
Joseph W. Thomas (P33226)
Attorneys for Plaintiff
2600 W. Big Beaver Road, Suite 550
Troy, MI 48084
Telephone: 248.649.6000
Fax: 248.649.6442
rtomlinson@driggersschultz.com

Dated: April 26, 2010

**CERTIFICATE OF SERVICE**

I hereby certify that on April 26, 2010, 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) and Lara Lenzotti Kapalla (P67667).

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