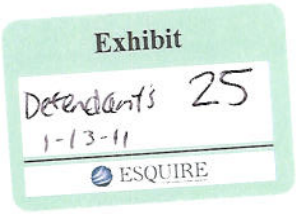
EXHIBIT B



REPORT OF LANCE JAMES

INTRODUCTION

My charge from Driggers, Schultz & Herbst was to examine the practices of Comerica Bank with respect to the acceptance of Wire transfers through their e-banking system and provide my opinion as to whether Comerica Bank (the "Comerica") acted in good faith and whether its conduct met industry standards in the accepting the on-line wire transfer charges to Experi-Metal's accounts in their e-banking system.

INDUSTRY STANDARDS

The industry standards that apply to the bank are derived from several sources, including the Gramm-Leach-Bliley Act of 1999, ("GLB") which requires the protection, confidentiality, and integrity of customer information; and the Federal Financial Institution Examination Council's Information Technology Examination Handbook. Section 501(b) of GLB required the development of Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "GLB Guidelines" attached as Exhibit 1). The GLB Guidelines apply to Comerica because it is an FDIC insured bank. The Federal Financial Institution Examination Council ("FFIEC") is a formal interagency body empowered to prescribe uniform 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 among other. The FFIEC has promulgated its Information Technology Examination Handbook (the "FFIEC Handbook"). The E-Banking and the Information Security Booklets of the FFIEC Handbook are attached as Exhibit 2 and serves as a supplement to the participant agencies' GLB Section 501(b) expectations.

Pursuant to the GLB Guidelines, as implemented by the FFIEC Handbook, Comerica should understand that no single control or security device can adequately protect a system connected to a public network. The Bank should have mechanisms in place to reduce the risk of undetected system intrusions. Fraud screening is a mechanism for detecting system intrusions. Fraud screening includes intrusion detection systems for network and individual servers, automated log correlation and analysis and identification of operational anomalies. The Bank should also have a testing plan to test precautions. The Bank should also establish fraud detection controls that prompt additional review and reporting of suspicious activity (cite). Suspicious activity includes and unusual volume or size of funds transfers and unusual account activity initiated from a foreign internet address.

The FFIEC Handbook describes the following industry standards that apply to Comerica. Controls should not be assumed to be completely effective (FFIEC Handbook, Information Security/Information Security Risk Assessment, p. 3). A well planned and executed security monitoring program is sound industry practice and should be based on an assessment of risk of non-compliance or circumvention of the institution's controls (id.). Weaknesses in token systems include Man-in-the-Middle ("MIM") attacks (FFIEC Handbook, Information Security/ Security Controls Implementation, p. 4). The weakness to MIM attacks can be addressed through additional control mechanisms (id.). MIM attacks can be protected against through the use of public key infrastructure ("PKI") (id.). An effective control mechanism includes numerous controls to safeguard and limit access to key information systems (cite). Behavioral

authentication, or fraud screening, is another element of authentication. While behavioral authentication does not provide strong assurance of who an individual is, it may provide a strong indication that the authenticators presented are form an imposter (id. P.6). Behavioral authentication would include looking at the browser used and how long a session lasts.

The FFIEC Handbook in setting the industry standard states, "All authentication methodologies display weaknesses." Examples of weaknesses include MIM attacks. MIM attacks can be controlled by monitoring DNS servers, authentication of the device communicating with the server and use of PKI. Thus, the industry standard is that additional levels of security be included, in addition to a token, which address the known weaknesses. The additional levels of security include fraud monitoring and fraud screening as well as monitoring DNS servers, authentication of the device communicating with the server and use of PKI.

As more fully outlined in my Summary of Background (Exhibit A) and my *Vita* attached as Exhibit B, I have been working as an information security professional, and developed my expertise as a consultant in the area of electronic bank fraud over the past 10 years. In my experience, working as a security consultant to numerous banks and financial institutions, I have noted that the banks have developed and executed well planned security monitoring programs in accordance with the FFIEC Handbook.

REASONABLENESS OF INDUSTRY STANDARDS

The Guidelines developed pursuant to Section 501(b) of the GLB are reasonable because the GLB is federal law and the development of such guidelines was a requirement of such law. The FFIEC handbook sets reasonable industry standards because it is a federal body charged with developing guidelines to determine if banks are in compliance with federal law. Since agencies charged with enforcing federal laws have developed guidelines that seek to enforce federal law they are reasonable.

OPINIONS AND BASIS FOR OPINIONS AND DATA CONSIDERED

COMERICA DID NOT MEET INDUSTRY STANDARDS

1. **Comerica did not meet industry standards in that Comerica did not have monitoring systems in place to detect unusual activity in Experi-Metal's accounts.**

Based on the testimony of Comerica employees and an analysis of wire activity in the Experi-Metal accounts at Comerica on January 22, 2009, Comerica did not meet the industry standard for the following reasons:

Comerica did not have monitoring systems in place to detect unusual activity in the Experi-Metal accounts: there was no fraud screening, no fraud scoring, Comerica did not address a known weakness to MIM attacks, there was no PKI in use, no monitoring of DNS servers, no authentication of the device communicating with Comerica's server and no evidence of testing Comerica's system. The Bank in fact had previously had PKI technology in place and removed it, thus making the Experi-Metal account more susceptible to a MIM attack.

Almost all financial institutions have adopted the industry standards and implemented monitoring systems dubbed "fraud scoring" or "fraud screening." Generally, this process is established by using readily available software indexing historic transaction patterns and then comparing those patterns against current activity through monitoring of current activity. The software then assigns higher scores to activity that does not match the normal spectrum for the particular account involved. At a certain threshold, the system alerts the bank to the unusual activity and the bank would freeze the activity to stop the suspicious wire transfers. These systems that have been implemented by the financial institutions measure variables such as the source IP address, session length, cookies, transaction speed, transaction amount, new transactions, destination bank locality and destination account name.

Examination of the Experi-Metal wire transfer web logs provided by Comerica (Exhibit 3) makes it quickly apparent that based on session length and the amount of wire transfers alone, any properly configured, industry standard monitoring device would have detected this activity almost immediately as being highly suspect. An example graph of regular activity performed by Experi-Metal two-days prior to the incident distinctly demonstrates the contrast when compared to January 22nd, 2009.

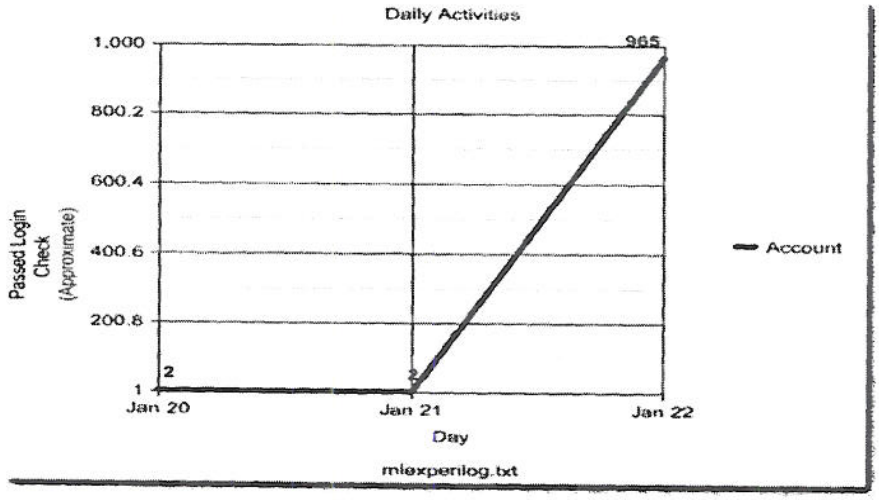


Figure 1 Jan 20-22nd 2009 Passed Login Check Activity

According to the logs provided by Comerica, online activity presents an average of two "Passed Login Check" (PLC) per day conducted by the Experi-Metal user account. A PLC is designed to validate logins when certain areas of the website are requested, such as the main login screen, ACH or Wire transfer templates. It simply validates the users' authentication and grants admittance in this area of the website for the existing session. On average, the legitimate use of the Comerica account and its website was rather minimal, and the session times ranged between two minutes and fifteen minutes maximum. On the days of January 20th through 21st, there were a total of four PLC that occurred with the account. The controller for Experi-Metal can testify that he logged in on those days and conducted minimal activity. However, on January 22nd, 2009 PLC activity exceeded over 900% compared to the previous two days.

Comerica has previously touted its monitoring capabilities in the press. In the fall of 2007, Comerica's Chief Technology Officer George Surdu states in an "Innovative Business Solutions" magazine interview:

"We have detection technology in place that can sense unusual or inappropriate activity and immediately alerts us to the issue."

Further investigation indicates that not only were the two days prior to the attack reasonably quiet and ***usual*** but evidence from Experi-Metal's bank statements specifically confirms almost no wire transfer activity in general.

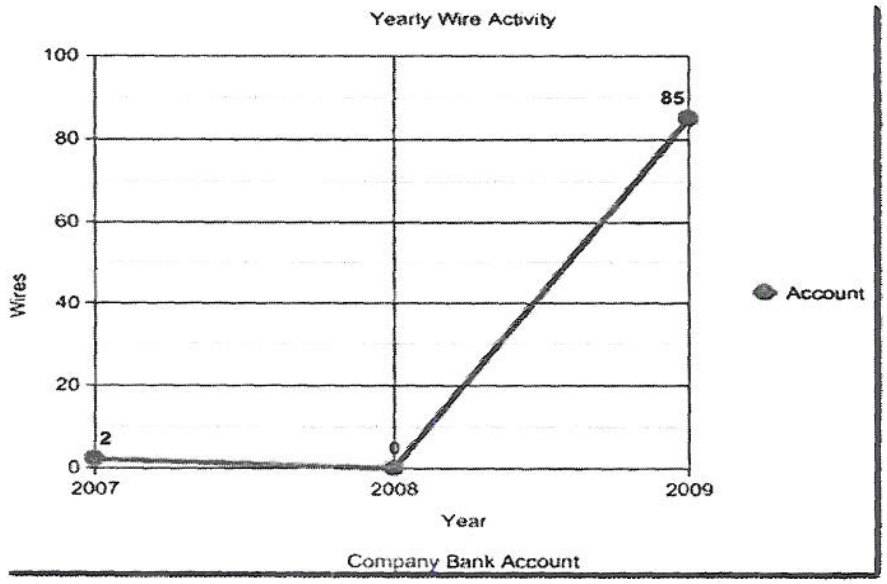


Figure 2 2007-2009 Wire Transfer Activity

In 2007, Experi-Metal conducted two wire transfers. A domestic (local) wire in June 2007 in the amount of $100,000.00 USD and an international wire transfer in May 2007 for $9,517.01 USD. In 2008 the company did not make any wire transfers. On January 22, 2009, 85 wire transfer requests (domestic and international) were made, again clearly marking a very definitive difference when analyzed against the two-year preceding pattern of the online account.

Given a worst-case example, such as a primitive fraud-monitoring device that only archives one previous year's history (2008) for the account, it is still very difficult to understand how the fraud that occurred could not have been detected within the first few minutes on January 22nd, 2009:

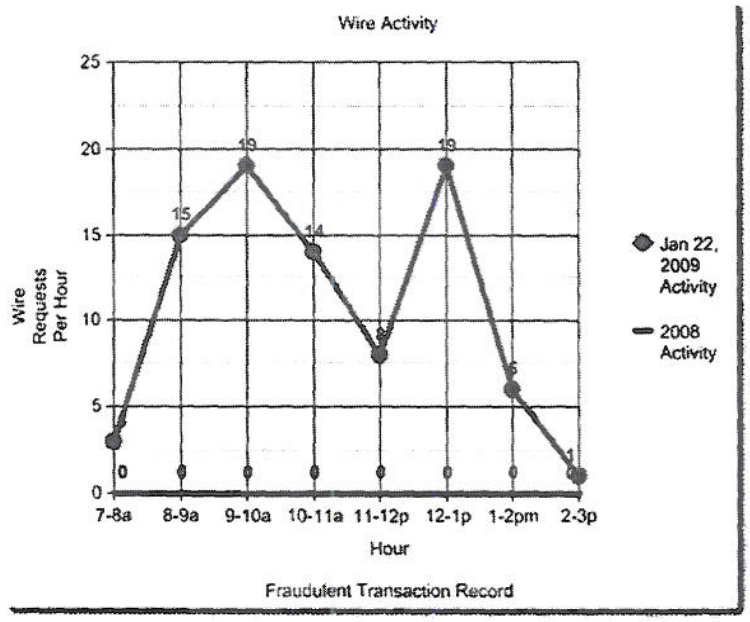


Figure 3 2008 Wire Transfers vs. Fraud Wire Transfers

Within the hour of 7-8am on January 22nd, there were three wire transfers initiated. Properly implemented monitoring would detect this, since there hasn't been a wire transfer from the account within the previous year thus it would immediately score these requests as suspicious activity. Most implementations also validate any new wire transfer destinations. This would halt the process until validated by the customer. If that were the case, this attack would have not been successful and Experi-Metal would have been notified immediately. Within minutes, a basic fraud monitoring system would have halted all wire-transfers as it was obvious this was ***unusual*** activity and Experi-Metal would have been notified. The third hour peeks the amount of wire transfers per hour at 19. It's not until into the 4th hour that Denise Ling from Comerica contacts Experi-Metal to inquire about the outgoing wire transfers, which at this time more than 60% of the eighty-five wire transfer requests were already performed.

When investing in anti-fraud software, specifically in regards to financial institutions, a key feature within the technology focuses explicitly on transaction amounts. If transaction amounts (be it wire or purchase) are unusual compared to the historical pattern, then an alert is triggered and preventative action is taken. Below is a graph focused on the wire transfer transaction sums historically. It would be safe to say anything even exceeding a transfer request of over $150,000.00 USD would be unusual for Experi-Metal. For this purpose the graph demonstrates a peek maximum of $1,000,000 US demonstrating the overly exceeded and undetected transaction amounts within the first three hours of attack prior to Comerica contacting the client.

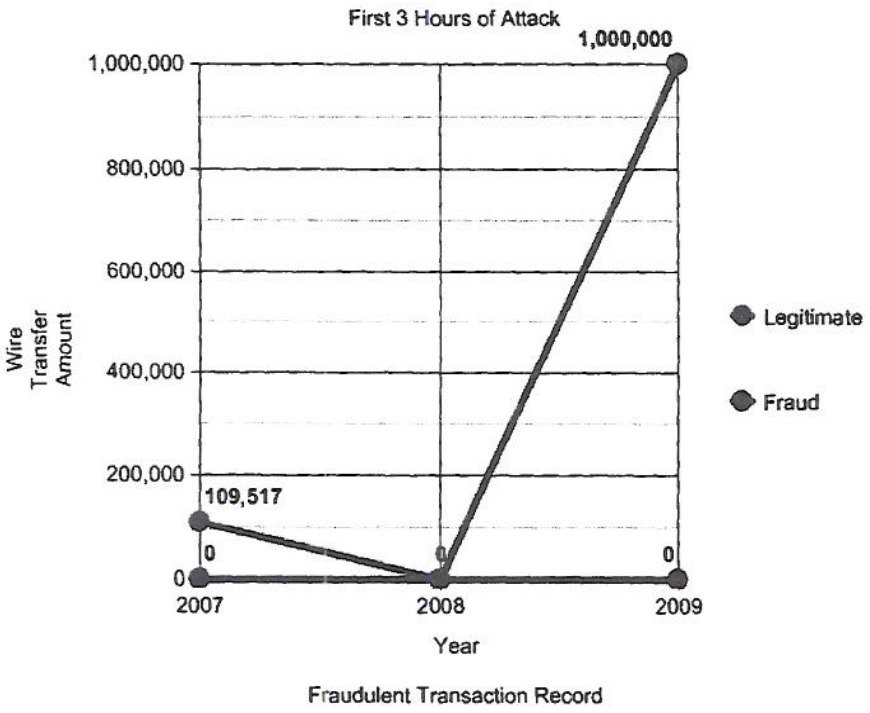


Figure 4 2009 Fraud Attack Transaction Analysis

According to the wire transfer records that were logged on the 22nd of January 2009, there were more than 25 requests to commence international wires. Accompanied with the wires are the names associated with the accounts. Many of the names are foreign in nature such as:

Darya Dulenko – Bank Moscow
Dmitri Kucherov – Alfa Bank, Moscow
Ekaterina Danilova – Bank Moscow
Igor Nosov – Lloyds TSB Scotland
Alexey Siverin – Bank Moscow

The names and destinations are acutely unusual given that any wire transfers that were initiated legitimately (prior to the attacks) have been sent only to business accounts and never to Estonia or Russia (high profile locations known for money laudndering).

The session length is also atypical for Experi-Metal's online account: Six hours of wire transfers without a session timeout. This manner of consistent activity for that timeframe is usually suspect in general.

A simple browser cookie check would also have alerted general anti-fraud software since the foreign computers accessing the account did not have the same cookies as the legitimate client computer. A new set of cookies for this account would be issued to the attackers' computer(s) and in effect would be considerably marked as suspicious.

These criterion are components that exist in fundamental anti-fraud software implementations. What is not available at this time is the foreign IP address address logs that display access to the January 22nd web session. There is a strong probability that those IP's were either international, or at the very least unknown to access this account prior to the 22nd. There is one central client computer that logs into the account at Experi-Metal and it will likely have the same IP, or a related IP in accordance with the Internet Service Provider that services the company office Internet. Had the Digital Certificate been available along with the 2-factor authentication, foreign IP's would have not been able to access the account, and the authentication mechanism would have protected Experi-Metal from the attack. Since that was not the case, the next level of protection should have been fraud-monitoring of the wire transfers instituted within the account. This also failed and was not able to protect Experi-Metal from losing a substantial amount of funds.

In my opinion, Comerica did not meet good faith or industry and commercial standards in that Comerica did not employ any type of monitoring system incorporating fraud scoring or fraud screening to detect suspicious or unusual activity. The answers to interrogatories demonstrate that Comerica did not have fraud screening or fraud scoring in place and did not address a known weakness to a man-in-the-middle-attack, there was no PKI in use, no monitoring of DNS servers, no authentication of the device communicating with Comerica server, and no evidence of testing Bank systems.

As a result of Comerica's lack of good faith, the fraudsters were able to log in and make over 85 fraudulent wire transfers from Experi-Metal's bank accounts to many overseas locations over a 7-hour period. If Comerica had complied with good faith and industry standards, Comerica would have quickly detected the fraudulent and suspicious activity within the first few transactions that were attempted by the fraudster. This is especially true since on January 21, 2009, Comerica had advance notice of an on-going phishing attack.

Comerica's lack of monitoring is further demonstrated by the actions of J.P. Morgan Chase and Bank of New York. Wire transfers from Experi-Metal's accounts were directed through these two banks intended for banks and accounts in Moscow. Although receiving only a few of the wire transfers, these banks quickly noted the suspicious activity associated with the wire transfers and alerted Comerica to the suspicious activity.

2. Comerica did not act in good faith and in compliance with its security procedures and any written agreements when it accepted the wire transfers initiated by the fraudster using Keith Maslowski's log in information.

In reviewing this issue, I have examined the written agreements between the parties with respect to wire transfers including the following:

- Treasury Management Services Agreement Comerica NetVision Wire Transfer dated November 21, 2003 (Plaintiff's Deposition Exhibit 2);
- Treasury Management Services – Implementation Worksheet dated November 25, 2003 (Plaintiff's Deposition Exhibit 3);

- Global Wire Transfer Authorization and Security Procedures dated November 1, 2007 (Plaintiff's Deposition Exhibit 4);

- Declaration for Entering Wire Transfer Agreements and Designation of Authorized Agents dated December 1, 2007 (Plaintiff's Deposition Exhibit 5);

- Comerica Bank – Wire Transfer Authorization and Security Procedure with No Call Back (Plaintiff's Deposition Exhibit 5);

- Comerica's letters to Experi-Metal dated April 25, 2008 and April 28, 2008 (Plaintiff's Deposition Exhibits 8 and 9);

- The deposition testimony of the witnesses in this case.

Based on the documents I have reviewed, and my background, education and experience, it is my opinion that Comerica did not act in good faith and in compliance with industry standards or its own security procedures and the written agreements between the parties when it accepted the wire transfers initiated by the fraudster using Keith Maslowski's log in information.

The agreements between the parties show that as of December 1, 2007 (Plaintiff's Deposition Exhibit 5); there was a written agreement between Experi-Metal and Comerica that there were only two agents of the Company who were authorized to initiate wire transfers. Under the written agreement between the parties, the two authorized wire transfer initiators as of December 1, 2007, were Valiena A. Allison and Gerald King. As of December 1, 2007, there were no other individuals who were authorized by the Company to initiate wire transfers. Although Keith Maslowski may have had some prior authorization to initiate wire transfers, the Agreements dated December 1, 2007 eliminated his authority and he was not given any such authority.

Comerica's subsequent correspondence dated April 25, 2008 and April 28, 2008 identified Valiena Allison and Keith Maslowski as "users" of the TMC Web but they contained no indication that Maslowski was an authorized wire transfer initiator for Experi-Metal.

It is my opinion that Comerica's actions in accepting the wire transfers and the payment order based on use of Maslowski's user information by the fraudster not only failed to comply with the agreements between the parties but also failed to comport with industry and commercial standards of the banking industry. Based on my experience with the banking industry, industry standards require written authorization from the customer before accepting a wire transfer initiated by an employee of the company. Comerica has been unable to produce any written agreement authorizing Keith Maslowski to initiate wire transfers after December 1, 2007. The banks do not accept corporate wire transfers unless the initiator of the wire transfer has been authorized, in writing, by the company as an initiator of wire transfers. This industry practice protects both the bank and the customer and protects against payment orders being accepted in circumstances where the individual initiating the wire transfer is not authorized by the company to initiate wire transfers.

3. Comerica did not act in good faith and in accordance with industry standards when it failed to take steps to protect and to warn its customers as to the phishing emails being sent to Comerica's customers.

The depositions of Scott Vowels and Anne Goldman, as well as certain exhibits (Plaintiff's Deposition Exhibit 61), show that Comerica was well aware that phishing emails were being sent to Comerica's customers as of the morning of January 21, 2009. Despite the fact that Comerica was well aware that phishing emails were being sent to its customers, Comerica failed to contact its customers in order to warn them of the fact that phishing emails were being directed to customers and the heightened risk of phishing attacks.

Phishing attacks have become far more common over the last 10 years. Professional security personnel that work for the banks are members of and participate in Internet groups designed to quickly convey information about phishing attacks so that counter measures and security measures can be taken by the bank in order to reduce the risks to its customers.

Industry standards have developed whereby the banks quickly notify their customers of the imminent threat of known phishing emails and potential phishing attacks directed to the banks' customers. Under the industry standards, when the bank is alerted to such a threat, the bank immediately contacts its customers advising of those phishing emails directed to its customers and warns the customers to protect against emails asking for customer information.

I have found evidence that indicates that this industry standard with respect to warning of customers is a standard that has been followed by Comerica in the past. Documentation indicates that on or about April 27, 2008, Comerica received information on the Internet that suspicious emails were being directed to its customers (attached as Exhibit 4). The Treasury Management Department provided written notification to Account Officers, including Claudia M. Cassa, who was the Account Officer for Experi-Metal's account. The account officers, including Ms. Cassa, then prepared warnings and sent them out to each of their customers in order to alert them to the phishing email being directed to customers and to alert them to the risk. A copy of the warning sent to Experi-Metal in 2008 in accordance with industry standards is attached (Plaintiff's Deposition Exhibit 13).

Unfortunately, Comerica failed to follow the industry standard or its own standard in January, 2009 and no warning was sent to Comerica's customers. Comerica's failure to follow its own procedure and industry standards shows a lack of good faith in this case.

4. Comerica did not act in good faith and in compliance with its security procedures in any written agreement when Comerica allowed the fraudster to transfer non-existent funds from a zero balance account into Experi-Metal's sweep account in order to fund the continuation of the unauthorized wire transfers.

Comerica's records (Plaintiff's Deposition Exhibit 25) show that Comerica permitted the fraudster to transfer non-existent funds from a zero balance account into Experi-Metal's sweep account and thereby fund the continuation of the wire transfers. If the transfer of the non-existent funds had not been accepted by Comerica, the sweep account would not have had any balance in it after 9:00 a.m. and no further wire transfers could have been accepted or paid.

Instead, for some unexplained reason, Comerica accepted transfers by the fraudster from the zero balance employee savings account into the sweep account, thereby allowing the fraudsters to continue to make unauthorized wire transfers. Interestingly, Comerica refused to allow transfers from some accounts but allowed transfers from a zero balance account with no funds in it.

Under industry standards, banks would not permit the transfer of non-existent funds and the wire transfers would have stopped. The only exception to this standard is if the customer has a written agreement with the bank to allow for such transfers or such payments in the absence of the required funds. Experi-Metal had never authorized these types of transfers from the zero balance employee savings account and had never authorized the transfers of non-existent funds to be honored by the Defendant. In fact, the evidence demonstrates that Comerica had followed industry standards in the past, and had not allowed Experi-Metal to transfer funds from accounts with insufficient balances (Plaintiff's Deposition Exhibits 6 and 7).

5. Comerica failed to act in good faith by failing to report the suspected fraud on a timely basis.

The documents in this case show that Comerica's wire room was alerted to the fact of the fraudulent and suspicious nature of the fraudster's fraudulent wire transfers from Experi-Metal's account and failed to respond to and report the information in a timely fashion.

J.P. Morgan alerted the wire room to fraudulent and suspicious activity with respect to these wires after six wire transfers had been sent to J.P. Morgan intended for accounts in Moscow. Comerica's records reveal that all six of these transfers were completed by 8:18 a.m. on January 22, 2009. The wire room at Comerica failed to report J.P. Morgan's notification of the suspicious and possibly fraudulent activity with respect to Experi-Metal's account to the Treasury Management Department until 11:39 a.m. that morning. The delay in reporting the fraudulent and suspicious activity is not in good faith and not in accordance with industry standards. Industry standards require that such activity be reported as soon as it is discovered.

6. Comerica did not act in good faith in accordance with industry standards when the fraudulent activity was reported to the Treasury Management Department.

The evidence (Rita Pniewski deposition testimony at p. 113) shows that at some time prior to 11:59 a.m., Rita Pniewski of the Treasury Management Department contacted Connie Jernigan and instructed her to disable the TMConnect Web and remove all access from the user. This required Jernigan to "kill the session" so that anybody that was currently on-line would be knocked off-line immediately. The evidence shows that Jernigan failed to follow her own department's procedure and failed to kill the session, thereby enabling the fraudster to continue on-line making fraudulent wire transfers. The documents show that Jernigan failed to follow her own procedures, and did not kill the session until approximately 2:05 p.m. that afternoon, allowing the fraudster continued access and a continuation of his wire transfer session. Obviously, Jernigan's failure to follow procedures or direction is a clear violation of not only Comerica's internal procedures but industry standards. When standards are developed they are meant to be followed and the failure to follow those standards is a clear violation of industry standards.

7. **Comerica did not act in good faith and in accordance with industry standards with respect to the wire transfer room accepting payment on a wire transfer after discovery of the fraud and after the wire transfers had been flagged and stopped at the wire transfer room.**

The documents in the case (Plaintiff's Deposition Exhibit 23 and the deposition testimony of Sean Murphy) show that the wire transfer room flagged all outgoing wire transfers as of approximately 12:25 p.m. on January 22, 2009. Under written instructions from the Treasury Management Department, no further wire transfers were to be accepted or paid.

The evidence shows that after the instructions from Treasury Management and after the wire transfer room had flagged all outgoing wire transfers from Experi-Metal's account, the wire room accepted payment of another wire transfer and released it from the wire transfer room ignoring the flag and the instructions at approximately 1:21 p.m. (Plaintiff's Deposition Exhibit 33). As a result, the wire was paid and the money was never retrieved. Comerica's action with respect to this particular wire obviously violated Comerica's standard as well as industry standards with respect to the payment of the wire transfer.

EXHIBITS THAT MAY BE USED TO SUMMARIZE OR SUPPORT OPINIONS

Depositions and all exhibits related to the depositions taken in this matter, exhibits attached and/or referenced in this report, and demonstrative exhibits.

QUALIFICATIONS INCLUDING ALL PUBLICATIONS AUTHORED IN THE LAST 10 YEARS

These are contained in my *Vita/Resume* attached to this report as Exhibit B and also to the summary attached as Exhibit A.

LIST OF ALL CASES IN WHICH I TESTIFIED OR WAS DEPOSED (PREVIOUS FOUR YEARS)

Testified in the United States House of Representatives on Bill HR 5136 on the security of U.S. telecommunication systems and regulations to assist in the prevention of severe criminal and/or terrorist activity.

STATEMENT OF COMPENSATION

I am compensated at the rate of $350 an hour for my work and testimony in this case. All travel related expenses are compensated separately.

Dated: January 6, 2011