

R. F. Cross, CPP

Wire Transfer Fraud Alert

An ASIS White Paper

July 2010

Wire Transfer Fraud Alert

Abstract: Small and medium size businesses and local governmental entities are incurring significant dollar losses due to wire transfer fraud. The Internet Crime Complaint Center (IC3) reported in October 2009 there had been approximately \$100 million involved in these fraudulent wire transfers. Courts may affirm banks not liable for business and governmental losses from wire transfer fraud. Uniform Commercial Code UCC4A and Federal Reserve System Regulation J establish legally binding protocols for wire transfers initiated by businesses and governmental entities. The FBI and the FDIC report a significant increase in wire transfer fraud where computer hackers, mostly from Eastern Europe and Russia, use malware to infect computers at a business, governmental entity, or bank. After hackers gain unauthorized access to an online deposit account, funds generally under \$10,000 are transferred to deposit accounts at banks in the United States; the latter belong to “money mules” who immediately transfer the funds to a foreign bank account. Typically, money mules receive a commission of eight percent and may be unaware of the fraudulent transfers. Most of the wire transfer fraud has involved single-factor authentication on the part of the requester and its bank, i.e., user name and password. Federal banking regulators have cautioned that the use of single-factor authentication as the only control mechanism to be inadequate for the movement of funds to other parties. A legally binding written agreement between business or governmental customer, their bank, and any third party acting on behalf of the bank, i.e., an ACH provider, should be executed to articulate security controls and protocols to include multi-factor authentication.

Copyright © 2010 by ASIS International

ASIS International (ASIS) disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

All rights reserved. Permission is hereby granted to individual users to download this document for their own personal use, with acknowledgement of ASIS International as the source. However, this document may not be downloaded for further copying or reproduction nor may it be sold, offered for sale, or otherwise used commercially.

The information presented in this White Paper is the work of the author, and does not necessarily reflect the opinion of ASIS, or any ASIS member other than the author. The views and opinions expressed therein, or the positions advocated in the published information, do not necessarily reflect the views, opinions, or positions of ASIS or of any person other than the author.

Is your business at risk because of your bank? Banks¹ where the victim businesses and governmental entities maintain their checking accounts are denying responsibility to reimburse their customers for fraudulent and unauthorized cash withdrawals. Stolen funds (estimated at over \$100 million in 2009)² are being electronically wire transferred between customer accounts at U.S. banks, and then transferred to accounts at banks located outside the United States. Substantial losses to victim businesses are forcing some businesses to terminate employees and/or enter into bankruptcy proceedings. To mitigate potential future fraudulent activity, strong legally binding security procedures need to be implemented by both banks and their customers.

A growing number of small and medium size businesses³ are incurring losses in hundreds of thousands of dollars due to wire transfer fraud. Typically, a computer hacker attacks a business that has an online checking account with its bank. The intruder gains unauthorized access to either a computer at the business or bank and obtains the user ID and password. The hacker sends multiple wire transfer orders payable to accounts at other distant banks in the United States or its territories where middlemen involved in the fraud, called "money mules," quickly wire the funds to a foreign bank for deposit into an account. Generally, cash transfer amounts are less than the \$10,000 Bank Secrecy Act currency transaction reporting requirements, however, in some instances, individual withdrawals may be over the \$10,000 currency transaction reporting requirement.

Courts May Affirm Banks Not Liable for Businesses Losses from Wire Transfer Fraud

Unlike consumers who are protected from electronic fraud loss by the Electronic Funds Transfer Act and Federal Reserve Regulation E, businesses may not have similar protection. UCC4A and Regulation J govern business wire transfer activity.

UCC4A, as adopted into State law, governs wire transfers, including automated clearing house (ACH) payment orders. UCC4A provides that 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 by the receiving bank is effective whether or not authorized, if 1) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders and 2) the bank proves it received the order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders in the name of the customer.

¹ The word "banks" as used in this document includes all financial institutions.

² See *IC3 Intelligence Note*, Nov. 3, 2009.

³ "Business" and "businesses" as used in the remainder of this document include governmental entities.

In legal cases where businesses have sustained financial loss from unauthorized fraudulent wire transfer withdrawals from their demand deposit banking accounts, UCC sections 4A-201 and 202 are applicable.

- In section 201, “a security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar devices.”
- In Section 202, “commercial reasonableness is a question of law to be determined by considering the wishes of the customer 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 to the customer, and security procedures in general use by customers and receiving banks similarly situated. A security procedure is deemed to be 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 authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.”
- There is debate concerning what is a commercially reasonable security standard for business wire transfers. Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. The author’s opinion is that single-factor authentication for wire transfer requests, including electronic, fax, telephone and person to person at a banking office, fails to provide commercially reasonable security protection to the customer. Further, it is believed that if single factor authentication (user name and password) case came before a court, it would be found not to be a commercially reasonable security procedure, whereas, use of multi-factor authentication security procedures for wire transfer requests have been found to be commercially reasonable by the courts.⁴

Regulation J is issued by the Board of Governors of the Federal Reserve System. It establishes rules and procedures for the collection of checks and other items by Federal Reserve Banks and funds transfers through the Federal Reserve Fedwire system that is owned and operated by the Federal Reserve Banks. It is used primarily for the transmission and settlement of payment orders governed by Fedwire and does not

⁴ See *Regatos v. North Fork Bank*, 5 N.Y.3d 395, 402 (2005) and *Braga Filho & Da Silva v. Inter Audi Bank*, U.S. District Court, S.D. New York, No. 03 Civ. 4795 (SAS).

include privately owned systems for making ACH transfers. Regulation J in Subpart B incorporates the provisions of UCC4A. In the event of an inconsistency between the provisions of Regulation J and UCC4A, the provisions of Regulation J shall prevail.

- The judicial system has affirmed in some cases that the banks involved in wire transfer fraud have no duty of care to their customers and thus, no financial responsibility to reimburse the victims for their loss. As an example in *Eisenberg v. Wachovia Bank*, The U.S. Court of Appeals Fourth Circuit ruled any state law that is either duplicative of or contradictory to Regulation J is preempted by latter. Further, the Fourth Circuit held that “Wachovia does not owe Eisenberg a duty of care” and “Eisenberg consequently cannot maintain a claim of negligence against Wachovia.”⁵

⁵ See 301 F3d 220 *Eisenberg v. Wachovia Bank Na.*

Public Warnings about Potential EFT Fraud

In a November 2009 press release, the FBI released the following:

“Within the past several months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium businesses, municipal governments, and school districts. In a typical scenario, the targeted entity receives a “spear phishing” e-mail which either contains an infected attachment, or directs the recipient to an infected website. Once the recipient opens the attachment or visits the website, malware is installed on their computer. The malware contains a key logger which will harvest each recipient’s business or corporate bank account login information. Shortly thereafter, the perpetrator either creates another user account with the stolen login information or directly initiates funds transfers by masquerading as the legitimate user. These transfers have occurred as both traditional wire transfers and as ACH transfers.”

The Internet Crime Complaint Center (IC3)⁶ advised in November 2009 that there has been a significant increase in online fraudulent wire transfers.⁷ The IC3 advisory noted the following:

- In most cases, the victims’ demand deposit accounts were at local community banks and credit unions, some of which used third party service providers to process ACH transactions.
- Mostly, the attacks infect the victim computers with malware that compromises the account holders’ Internet banking account.
- In some cases the involved banks and third-party providers neither had firewalls installed nor anti-virus software on their servers or their desktop computers.
- As of October 2009, there had been approximately \$100 million involved in these fraudulent wire transfers.

⁶ IC3 is a partnership between the FBI and the National White Collar Crime Center that serves as a means to receive Internet related crime complaints.

⁷ See *IC3 Intelligence Note*, Nov. 3. 2009.

The Federal Deposit Insurance Corporation (FDIC) has put the CEO of each FDIC insured financial institution on notice of an increase in schemes to recruit individuals to receive and transmit unauthorized electronic funds transfers (EFTs) from demand deposit checking accounts to individuals overseas. According to the FDIC:

- Funds transfer agents in the United States, often referred to as “money mules,” are typically solicited on the Internet by criminals who have gained unauthorized access to the online deposit account of a business or consumer. In a typical scenario, the criminal will originate unauthorized EFTs from a victim’s account to a money mule’s deposit account. The money mule is then instructed to quickly withdraw the funds and wire them overseas after deducting a “commission” (commonly eight to ten percent).
- Criminals target online deposit accounts at institutions where business customers can originate EFTs, such as automated clearing house (ACH) and fed wire transfers, over the Internet. Money mules, however, can be customers at any depository institution where EFTs can be received and funds withdrawn. In some cases, the money mule may be an unknowing accomplice in a fraud scheme as funds availability from EFTs are often made immediately available by the receiving institution. Thus, funds may be removed and wire transferred overseas before the fraud is detected.
- Money mule schemes can take many different forms, but most involve receiving unauthorized EFTs into a deposit account and then withdrawing the funds or forwarding them on to another party via another EFT. In the majority of cases, the final benefactors of stolen funds reside outside the United States and most probably in Eastern Europe.
- Money mule activity is essentially electronic money laundering addressed by the Bank Secrecy Act and Anti-Money Laundering Regulations. Strong customer identification, customer due diligence, and high-risk account monitoring procedures are essential for detecting suspicious activity, including money mule accounts.

EFT Security Risks

Single-factor authentication of customer requests to their banks for electronic funds transfer from checking accounts to third parties is an unacceptable banking procedure for both banks and their business customers. Businesses that use only a username and password for Internet electronic funds transfer are potentially exposed to unauthorized fraudulent money withdrawals from their demand deposit accounts by computer hackers, who use malware to install a key logger and gain access to computers used by either the customer or the bank.

- The Federal Financial Institution Examination Council and the four banking regulatory agencies⁸ issued in 2001 and again in 2005 guidance on authentication in an Internet banking environment that state in part, “The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the **movement of funds to other parties.**”⁹
- Businesses take note: If you and your bank agree in writing on single-factor authentication for wire transfer request processing to third parties and fraud occurs, you may be found legally liable in a court of law for any losses in accordance with UCC4A. According to 4A, any claim to your bank for loss must be made within one year of receiving notification of the funds transfer.
- Use of single-factor authentication by businesses and banks for electronic funds transfer has enabled hackers to commit account fraud. Several examples of successful electronic funds attacks follow:
 - A business computer at a clinic in Jacksonville, Florida, with fifty practicing physicians was compromised by malware with hackers gaining access to the log-in password and successfully wire transferred forty-four transactions from its business banking account totaling approximately \$430,000 to banks in Germany and the Netherlands. Each of the transactions was less than \$10,000 and below the Bank Secrecy Act currency transaction reporting requirements. The initial transfer requests were made to banks located in western U.S. Some of the transferred funds were reversed; however, the clinic sustained a loss of approximately \$300,000. The clinic’s bank is using UCC4A as a defense in denying financial responsibility for this loss.¹⁰

⁸ The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

⁹ Emphasis added by author.

¹⁰ Source: inquiry to the author for expert witness support from the clinic’s attorney.

- A business computer at a car dealership in Anchorage, Alaska had its banking account login and password compromised by hackers from Eastern Europe. The wire transfer loss to the car dealership was approximately \$100,000. The stolen funds were transferred in multiple wire transfers in amounts less than \$10,000 to numerous banks in the lower 48 states and then transferred by “money mules” to foreign bank accounts. The car dealership bank is using UCC4A as a defense to deny financial responsibility for this loss.¹¹
- The Western Beaver County School District in Pennsylvania is suing ESB Bank for executing 74 unauthorized cash transfers totaling \$704,610 over four days during the Christmas school break during 2008-2009. Court records show funds moved into 42 receiving accounts in several states and Puerto Rico. The bank recovered \$263,413, but is denying financial responsibility for \$441,197 claiming the school district failed to secure its computers. Attorney Brian Simmons of the Pittsburgh law firm Buchanan Ingersoll & Rooney representing the school district is quoted as saying “the school district would like its money back.”¹²

A Future National Strategy to Combat Online Fraud

Recently, the White House released a draft strategy for reducing cybersecurity vulnerabilities, such as identity theft and fraud.¹³ This strategy envisions the creation of an Identity Ecosystem where both public and private users will be able to securely authenticate themselves online for different types of transactions, including banking, through the use of trusted digital identities. It is noted this strategy emphasizes the importance of the identification, authentication, and authorization of each user transaction. Although, this is a positive step to enhance the security of business wire transfers, it may be several years before the necessary private sector hardware, software and/or federal regulation can be developed and implemented. Thus, it is essential businesses take immediate steps to minimize the potential of financial loss due to wire transfer fraud.

¹¹ Id.

¹² *USA Today*, “Cyber Crooks Stalk Small Businesses that Bank Online,” Bryon Acohido, Jan. 10, 2010. The author was retained as a bank security expert by the Western Beaver School District. A favorable settlement between Western Beaver and its bank was obtained.

¹³ See White House Blog on the National Strategy for Trusted Identities in Cyberspace posted by Howard Schmidt, June 25, 2010.

Procedures to Mitigate EFT Security Risks

When a business decides to engage in Internet electronic wire transfer activity through its bank to third parties, a legally binding written agreement between the business, its bank, and any third party acting on behalf of the bank (e.g., an ACH provider) needs to be in force. The written agreement should include the following recommended topics:

- Specify the type of funds transfer included (i.e., electronic, fax, telephone and/or person to person inside the customer's bank).
- Identify to the bank persons authorized to request a funds wire transfer.
- Provide the bank with signatures of customer employees authorized to request a funds transfer request to third parties.
- Specify the upper dollar limitation amounts and frequency of funds transfers.
- Specify the bank use of a two factor authentication for user login that must include two or more of the following: 1) something a person knows, 2) something a person has, and 3) something a person is.
- Specify the two factor security authentication procedure to be used by the bank and customer.
- Specify that both the bank and business customer must install a commercially reasonable security software suite to include antivirus, anti-spyware, and malware and adware detection from a reputable vendor.¹⁴
- Specify that both bank and business customer use a dedicated computer for all online transactions and implement white listing methods to prevent the system from going to any site/address that does not have a documented business need.¹⁵
- Establish with the bank a confidential security question for each person authorized to withdraw funds from the business account.
- If possible, specify the identities and geographical location of persons and/or business(es) who are to be payees at the receiving bank.
- Specify the bank is to use fraud detection software to alert when an unauthorized computer, unexpected IP address, or suspicious activity is detected.
- Specify the bank is to immediately report to the customer any suspicious account activity.
- Specify the bank and customer is to immediately report all suspicious account activity to law enforcement.

¹⁴ See "Cyber Security Advisory" issued by multiple entities including the Financial Services ISAC, dated Mar. 12, 2010.

¹⁵ Id.

As a final note, all wire transfer agreements entered into by the customer, its bank and/or third party provider should be reviewed by the customer's attorney prior to signing any acceptance contract.

Inquiries and/or questions concerning this paper may be directed to the author at:

Richard F. Cross, CPP

Bank Security Expert
333 Kiyuga Way
Loudon, TN 37774

865-458-8946
865-809-3338 (cell)
email: dickcross1@charter.net



1625 Prince Street
Alexandria, VA 22314-2818
USA
Phone: +1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org