JOURNAL OF ACCOUNTANCY

TECHNOLOGY

Guard Against Cybertheft

Learn steps that can help avoid falling victim to electronic funds transfer fraud.

BY TOMMIE SINGLETON, CPA/CITP/CFF, PH.D. AND STEVEN J. URSILLO JR., CPA/CITP

OCTOBER 2010

A type of fraud has come into the public eye in the past year in which the criminal surreptitiously obtains financial banking credentials, hijacks a corporate computer, and steals money from the victim's bank accounts.

In this scenario, referred to as a fraudulent electronic funds transfer (EFT) transaction, a cybercriminal uses a software tool to gain control of the victim's computer from a remote computer. The criminal then uses an EFT to move most, if not all, of the money in the victim's bank account to one under his or her control, often costing the victim tens, if not hundreds, of thousands of dollars. The increasing scope of this fraud prompted the FDIC to issue an alert warning about it last year (available at tinyurl.com/2cz9sto).

According to the FDIC alert, the number of frauds has increased, as well as the size of losses, resulting from cyberthieves' stealing login credentials and using them to carry out unauthorized EFTs, which include Automated Clearing House (ACH) transactions and wire transfers.

Many small to medium-size businesses (SMBs) face some risk related to this fraud. *The Washington Post* reported a case in November 2009 in which cyberthieves tried to steal $1.3 million from a large property management firm by initiating debits against it with credentials stolen from a painting company.

What makes this type of fraud a widespread concern for CPAs is that, rather than targeting large banks, criminals are targeting businesses that may be clients of public accounting firms. Additionally, CPAs who work in business and industry are often in a key accounting position or are the finance officer, and thus are in positions of responsibility related to this type of fraud.

This article describes how these crimes are perpetrated, the associated risks and some preventive measures.

A TYPICAL SCENARIO FOR EFT FRAUD

In a legitimate setting, a bank's customer who has established the ability to conduct online EFT transactions connects to a financial institution to execute a wire transfer or ACH transaction. The expectation is that the customer's system, once authenticated by the bank, is authorized to conduct the activity. However, in the case of this particular EFT fraud, a cybercriminal compromises the originating system. There are many types of EFT fraud, but this article is limited to the specific scheme described in this section, primarily wire transfer fraud, but also ACH transaction fraud.

Time is of the essence in discovering and responding to unauthorized EFT transactions. Unlike the case with consumers, who enjoy strong federal protection in cases of ACH fraud, a business must notify the bank within two days of a fraudulent ACH transaction or the business may be liable for the loss. But a fraudulent wire transfer demands detection within hours—less than two days.

The scheme has basically three steps: (1) illicitly acquire the login credentials, (2) covertly gain unauthorized access to the victim's computer to avoid the bank's security features that are activated when it does not recognize the login "fingerprint," and (3) transfer the victim's bank funds to an account the cybercriminal controls.

In the first step, credentials are usually compromised by using a malicious program distributed as an e-mail attachment, unintended Web browsing download, or file transfer of a seemingly legitimate/ innocent file. The user inadvertently allows this malicious program (for example, a "Trojan horse") to be downloaded and executed. The attacker then can use the program's keystroke-capturing functionality to capture the organization's bank account information, banking credentials, and online activities (for example, EFT transactions). The user of the compromised computer is usually unaware that anything malicious has occurred.

Bank security systems use a technique that can be described as a "fingerprint" to authenticate customers for online banking. It is basically a snapshot of one or more computer/IT features such as an IP address, cards attached internally to the computer, and other technical aspects of the system that are accessible from the computer's memory. Those are read by the bank's system to create a relatively unique set of technology features. The fingerprint is saved when the customer registers with the bank. At any login, the bank's authentication system takes a snapshot of the computer logging in to the system, matches that fingerprint against the one on file, and if it is substantially the same, the system assumes the user is authentic. If it does not match, the bank's authentication system adds a layer of authentication by asking a security question or using an alternative authentication procedure (for example, a personal identification number (PIN) sent to a previously arranged cell phone or e-mail account)—which again was established by the customer during the account setup process.

In the second step, the cybercriminal hijacks the victim's computer system to use it as a trusted source to avoid the security of the fingerprint, and to allow the fraudster to conduct a fraudulent EFT. The criminal uses a hacker tool (software) to hijack the system. If the criminal simply stole the credentials and tried to log in from his or her own computer, that would lead to another layer of authentication (that is, fingerprints do not match) that the criminal would likely be unable to compromise. But the bank's system recognizes the login from the victim computer's fingerprint, does not sense a need for further security measures, and mistakenly allows the unauthorized user to access the account.

Once logged in and authenticated by the bank's security system, the criminal proceeds to the last step. He transfers out most, if not all, of the funds in the victim's bank account, usually via wire transfers, and typically sends the funds to individuals known as "money mules." Mules are often recruited through common online help-wanted job sites, and, in most cases, are unaware that the activity they are performing is related to a crime, usually under the impression that they are working for some legitimate business, such as a marketing company.

The criminal wires the mule amounts just under $10,000, to avoid Bank Secrecy Act requirements to file a Currency Transaction Report (CTR) for deposits of $10,000 or more and thus avoid potential immediate detection. The mule is instructed to keep a small amount (usually $500 or less) as compensation, and then to transfer the remainder to an account specified by the criminal. That account is typically an offshore account in a safe harbor for the crook (for example, the funds may be transferred to a foreign country uncooperative with the FDIC and U.S. banks, such as Latvia or Ukraine), usually preventing recourse by the bank to recover the funds.

The primary hope of recovery is that the bank will be able to reverse the wire transfer. The Uniform Commercial Code (UCC) requires banks to make a best effort to recover the funds. But there is a catch: Section 202 of Article 4A of the UCC says that "a payment order received by the … bank is effective as the order of the customer, *whether or not authorized*, if … the bank proves that *it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer* …" (emphasis added).

If the fraud can be traced to a security breach in the victim's computer (for example, malware or hijacking program), the bank may be able to avoid responsibility for the recovery of the lost funds. The bank also may find that the customer is not in compliance with its security authentication procedures, which also impairs the victim's ability to recover lost funds. The bank must explicitly agree in advance to be liable for damages from EFT fraud before recovery is generally possible. Even if the bank makes a best effort to recover the funds, it may be impossible for the bank to recover anything, leaving the victim to suffer the loss. Therefore, the bank seldom gets stuck with a loss from this EFT fraud. Even lawsuits by victims against banks are difficult because of the UCC rules, the fact one cannot sue the overseas bank involved, and the resistance likely to be encountered by the bank's attorneys.

Wire transfers are difficult to recover because they are instantaneous, basically treating the nonconsumer customers as a bank and sending the money directly into an account. A wire transfer fraud can go from the victim's bank, through an intermediary account, and end up in an overseas account within a few minutes. ACH transactions usually take a day or two because of the "float" that generally happens due to the intermediary "clearinghouse" used to complete the transaction.

RISK ASSESSMENT OF EFT FRAUD

EFT fraud prevention steps share a commonality with general fraud prevention. The organization should conduct a formal risk assessment including the specific activities around the EFT processes, and then develop policies, procedures and controls around the relevant risks.

The risk assessment should include determining if a reliable recourse for recovery exists if an EFT fraud occurs. For instance, can the entity detect an unauthorized wire transfer quickly, and respond in a short time frame? Is the entity in compliance with the bank's recommended security procedures to facilitate recovery? Does the entity have the type and level of insurance protection for this type of crime? That is, what is the maximum dollar amount the entity could lose in a wire transfer, and does the business insurance cover that amount for fraud? Usually the maximum coverage amount would be the highest balance in the bank account where wire transfers are conducted. It also should take into account the business processes, policies, procedures and controls associated with online banking.

Has the entity communicated and cooperated with the bank to develop sufficient policies, procedures and controls to avoid this type of fraud? Has the entity given proper education and/or training to key employees—those with online access—so they understand the risks, how the fraud is perpetrated and the countermeasures they should take as individuals? What are the current controls? How does the entity prevent malicious code (malware) from being installed onto its systems? What controls does the entity have to prevent computers from being hijacked?

Once the relevant risks and vulnerabilities have been identified, and a risk level has been determined, the organization can begin to identify controls that will mitigate the risk (see Exhibit 1 for a summary of additional controls).

Exhibit 1: Controls for EFT Fraud

- Dedicate a computer or system for online banking, especially EFT (ACH transactions and wire transfers).
- Use multifactor authentication with independent mechanism (for example, require login credentials *and* a temporary PIN sent to a pre-determined cell phone or pager device; login credentials plus swipe card; etc.).
- Log and monitor key computers or systems.
- Segregate EFT controls. For example, one person performs online EFT function (ACH transactions and wire transfers), and a second person approves the transfer or verifies/reconciles that transaction.
- Reconcile EFT transactions daily.
- Dedicate clearing accounts using “just-in-time” deposits. For example, set up a separate bank account for EFT transfers (ACH transactions and wire transfers), and make deposits (or online transfers from a different computer) into that account just before a wire transfer occurs. The risk is limited to a very brief time frame when money is available in the clearing account.
- Use a “run as needed” bootable CD (such as the Ubuntu operating system) that cannot be contaminated by a virus or malware for the computer accessing online EFT. This is an FDIC recommendation.

PREVENTING AND DETECTING EFT FRAUD

Controls designed to combat the prevalent distribution of malware should also be considered. All systems, especially the computer used to conduct online banking, should be protected by a firewall and monitored with updated antivirus and malware protection. Access to online banking computers should be based on least privilege (that is, “need to know,” limited access), incorporating all the proper physical and logical access controls, including account policies.

If the organization determines that EFT fraud poses a significant risk based on the nature of the business conducted, consideration can also be made to use dedicated computers, systems and/or networks for EFT activity. A dedicated computer potentially serves as an effective preventive control over EFT fraud. Dedicated systems should also *not* be used for e-mail, Web browsing, or other high-risk online activities associated with contracting malware infections, but only for online banking. In addition, all critical activity around this system should be logged and monitored. When combined with a reasonable firewall on that computer, this scenario virtually prevents EFT fraud.

A key to prevention is to have adequate protection against a malicious keylogger being planted on a computer. Company management should make sure that security software is updated. Firewalls must be able to detect viruses, spyware and other malware.

Transactional multifactor authentication delivered with an independent device (for example, a token or electronic key fob—a small device that is kept on a keychain that uses some electronic means to access something)—makes an attack more difficult because one of the authentication factors (the one-time password or PIN) is not communicated to the operator through the compromised computer. For example, the bank could communicate the temporary PIN through a prearranged pager device. This control depends on the features of the bank’s system.

The use of a dedicated clearing account is a known best practice to prevent frauds like this one when established by customary standards. The entity would establish a clearing account to do *all* EFT transactions, while also blocking all other entity accounts from doing *any* EFT transactions. Then by transferring just enough money to the dedicated clearing account for EFT/ACH/wire transfers, just in time for the online transactions, the entity can limit its exposure for the simple fact the account seldom has a significant balance of funds. Each control presents security in layers, so there should be separate channels for transfer authorizations and EFT transactions (not authorized from the same computer or account profile).

The organization should also consider additional operating controls and detective measures. These would include implementing proper segregation of duty with dual-control functionality—critical controls to have in any EFT process. An example of segregation of duties might be having one person make the wire transfers or ACH transactions, and another person approve them. For instance, the National ACH Association (NACHA) suggests that banks set up EFT transactions for their customers so that they involve two parties where one originates the transaction and a second person authorizes it. If that segregation is not possible from the bank’s system, then the entity could establish some internal segregation using the following procedure: (a) The first employee initiates the EFT transaction, (b) it is forwarded electronically to a second person’s computer (*must* be a different computer with different login credentials) who approves it, and (c) the transaction is then forwarded to the bank. If the entity’s system is not capable of this kind of electronic segregation of duty, a similar control could involve manually separating the process; for example, a second person could monitor all EFT activity each day from the previous day and reconcile the transactions to those that were authorized.

Regardless of segregation of duty, monitoring and reconciling EFT accounts daily is important to quickly identify unauthorized transactions, and to enable the entity to possibly reverse any fraudulent transactions. This type of control is clearly a detective one and not a preventive one. Positive pay (bank confirmation) can be a strong preventive control as well. Other preventive and detective control services can be designed in-house or provided by real-time risk management service providers. They include transaction verifications, controls totals, blocks and limits, predetermined risk velocities and customer process monitoring. For example, management should verify transactions daily, match the total transaction amount from the bank with their daily activity, set up limits and frequencies on the amounts being disbursed, in addition to using other business rules (duplicate checking, etc).

Responding to an EFT fraud may require both technical and operational expertise. Trojan horse programs used to perpetrate these crimes are often difficult to detect and remove. In addition, an in-depth understanding of transaction and data flow throughout the EFT process will play a critical role in discovery.

This type of fraud is a risk to many entities, and a special threat to smaller entities because of the possible financial damage it can do, and the fact that this group is the one most targeted by criminals conducting EFT fraud.

EXECUTIVE SUMMARY

■ **There has been an increase in electronic funds transfer (EFT) fraud** being perpetrated on small to medium-size businesses in the past year.

■ **Victim entities have their bank login credentials stolen** by cybercriminals, who then take remote and unauthorized control of the victim organization's computer, and proceed to transfer all available funds from accounts via wire transfers or Automated Clearing House (ACH) transactions.

■ **It is possible that a victim of this fraud will be unable** to recover lost funds.

■ **There are controls to mitigate the risk associated** with this fraud and the related losses, including appropriately designed policies and procedures, awareness/ education, information security controls and banking procedures.

■ **CPAs in public accounting should be aware** of this fraud so they can advise potentially affected clients.

■ **CPAs in business and industry have an even greater** interest in understanding this fraud to mitigate potential risk for their employer.

Tommie Singleton *(tsingleton@cricpa.com) is a scholar-in-residence at Carr Riggs & Ingram in Birmingham, Ala., and an associate professor in the Accounting & Finance Department of the University of Alabama–Birmingham.* ***Steven J. Ursillo Jr.*** *(sursillojr@sju.com) is a principal and the director of Information Technology and Assurance Services at Sparrow, Johnson & Ursillo Inc., a Rhode Island-based full-service CPA firm.*

To comment on this article or to suggest an idea for another article, contact Alexandra DeFelice, senior editor, at adefelice@aicpa.org or 212-596-6122.

AICPA RESOURCES

JofA articles

- "Firm Up Your Data Security," June 2010, page 18
- "What's Your Fraud IQ?" Jan. 2010, page 34
- "Guidelines Aimed at Thwarting ID Theft, Security Breaches Unveiled," Dec. 3, 2009, online only
- "Password Management Strategies for Safer Systems," July 2009, page 54
- "Managing Multiple Identities," Sept. 2008, page 38

Use journalofaccountancy.com to find past articles. In the search box, click "Open Advanced Search" and then search by title.

Publications

- *Financial Reporting Fraud: A Practical Guide to Detection and Internal Control*, 2nd edition (#029890)
- *The CPA's Handbook of Fraud and Commercial Crime Prevention* (#056504)
- Generally Accepted Privacy Principles (GAPP)
- SysTrust

CPE self-study

- *Internal Control and IT: Reliable Reporting and Fraud Prevention* (#732555SNF)
- *Revenue and Cash Receipts: Common Frauds and Internal Controls* (#753341SNF)
- *Purchasing, Inventory, and Cash Disbursements: Common Frauds and Internal Controls* (#753331SNF)

Conference

AICPA Controllers Workshop East, Nov. 11–12, Orlando, Fla.

For more information or to make a purchase or register, go to cpa2biz.com or call the Institute at 888-777-7077.

Websites

- AICPA Information Technology Center
- AICPA Anti-Fraud and Forensic Accounting Center

Other guidance

- *Incident Response Plan: Template for Breach of Personal Information*
- *Managing the Business Risk of Fraud: A Practical Guide*

FVS Section and CFF credential

Membership in the Forensic and Valuation Services (FVS) Section provides access to numerous specialized resources in the forensic and valuation services discipline areas, including practice guides, and exclusive member discounts for products and events. Visit the FVS Center at aicpa.org/FVS. Members with a specialization in financial forensics may be interested in applying for the Certified in Financial Forensics (CFF) credential at aicpa.org/CFF.

IT Center and CITP credential

The Information Technology (IT) Center provides a venue for CPAs, their clients, employers, and customers to research, monitor, assess, educate and communicate the impact of technology developments on business solutions. Visit the IT Center at aicpa.org/infotech. Members who want to maximize information technology to increase efficiency and boost profits may be interested in joining the IT Membership Section or pursuing the Certified Information Technology Professional (CITP) credential. For more information about the IT Membership Section or the CITP credential, visit aicpa.org/CITP.

OTHER RESOURCES

Website

FDIC Special Alert, SA-147-2009, Aug. 26, 2009

More from the *JofA*:

Find us on Facebook | Follow us on Twitter