P&C RISK REVIEW

A PUBLICATION OF THE PROFESSIONAL LIABILITY INSURANCE NETWORK

FINANCE INSURANCE, LTD.
Quality Service For Your Insurance Needs

VOLUME 007, 2013

For More Information Contact:
Alan Taguchi
Tel: 522-5580
Fax: 522-2082
email: ataguchi@financeinsurance.com

Preventing Electronic Funds Transfer Fraud

This material is provided for informational purposes only. Before taking any action that could have legal or other important consequences, confer with a qualified professional who can provide guidance that considers your unique circumstances.

Although online banking is a relatively recent phenomenon, it's already difficult to image life without it. For both personal and business banking, the ability to pay bills, collect fees and otherwise transfer funds from a remote computer virtually eliminate the need to visit a brick-and-mortar bank to make financial transactions.

Unfortunately, as an increasing range of financial transactions move to the virtual world of computers, a whole new set of liabilities arise. Chief among those is the fraudulent electronic funds transfer (EFT).

What Is Fraudulent EFT?

Fraudulent EFT is the activity of accessing a personal or business bank account and transferring the funds to another account without permission. Gaining access to an account can occur through various means. For example, someone can steal your credit or debit card, or copy your card numbers and passwords through a sophisticated reader illegally attached to an ATM machine.

For today's businesses, however, perhaps the greatest threat is having someone gain access to your online bank account and illegally transfer funds into their own account. One source of such illegal activity are dishonest company employees. There are many cases of employees who have access to company financial accounts ciphering company money by making payments to bogus vendor accounts they set up.

A bigger threat to companies, however, are fraudulent EFT's perpetrated by computer hackers, often located halfway around the world. These thieves can and do instantaneously empty a company's entire bank account, often resulting in losses of hundreds of thousands of dollars.

A Hacker at Work

How do hackers perpetrate such thefts? Here's a typical scenario:

A company employee -- say an accounting clerk -- receives an innocent looking email, seemingly sent by a trusted associate or even the company's bank. The email contains an attachment that appears to be an important file. The clerk opens the file and reads the attachment.

Unbeknownst to the employee, the act of opening the file launches a malicious program that is downloaded and executed on the employee's computer. The intruder now has access to, and often control of, the computer. It can track the employee's every move on the computer and capture his or her keystrokes. Soon, it has the URL's for all of the company's financial institutions as well as the usernames and passwords used to access the accounts.

With this information and the malware embedded in the company computer, the hacker can now hijack the employee's computer. It can access the financial accounts and, because the activity appears to be coming from the familiar company computer and network, the bank security system has no reason to believe this is fraudulent activity. The hacker can then begin moving company funds to other

bank accounts, often located overseas. Sophisticated hackers know how to disguise the location of their accounts and move the transactions through a series of computers, some perhaps hijacked from other companies, so as to hide the money trail. The next time an employee logs into the company's bank account, which may be days later for small firms, the company's money is gone and the trail is cold.

Some businesses mistakenly believe that it is the bank, not the company, that will foot most of the loss for fraudulent EFTs. But while an individual enjoys certain protections if a hacker drains his or her personal accounts, businesses are not so fortunate. Depending on the specifics of the case and the timeliness of reporting the fraudulent activity, companies can suffer most if not all of the loss.

Prevention the Best Medicine

Design firms need to take steps to prevent fraudulent EFTs. Among the recommended steps:

Formalize your EFT policy. Develop a strict policy regarding who has access and authority to make electron fund transfers. As a general rule, you want to limit who has access to company bank accounts as well as limit the number of computers that can provide access to company funds. At the same time, you don't want a single employee to have full authority over electronic funds transfers. It is usually best to have responsibilities divided so that oversight is in place.

Reconcile bank accounts frequently. The EFT policy should establish frequent reconciliations of all company bank accounts -- preferably daily -- so that any suspicious withdrawals are caught at the earliest time possible. Discovering fraud quickly is essential to possibly reversing the transaction and limiting the company's liability.

Upgrade computer security. Up-to-date antivirus software and adequate company firewalls are your first line of defense to combat malware and keep intruders out of your computers. Antivirus software helps detect and quarantine dangerous files and programs that can damage and control your computers. And don't forget physical security as well. Keep computers that access your bank accounts under lock and key when not in use. And make sure usernames and passwords are kept secure and frequently updated.

Insurance Is Your Final Safeguard

Hackers get more sophisticated by the day, and software and hardware protection has difficulty keeping up with the latest and greatest threats. Since you can never guarantee 100% protection of your electronic funds, insurance can be your last line of defense.

Funds Transfer Fraud insurance is a specific type of crime insurance. It is typically combined with Computer Fraud insurance in what is called a "wrap" policy.

It is important to note that while the Funds Transfer Fraud and Computer Fraud insurance agreements may contain similar coverages, there are important differences. Namely, the Funds Transfer Fraud coverage specifically protects against losses caused by fraudulent instructions given to the financial institution by a third party and purported to have been sent by the insured to transfer, pay or deliver funds to another account. This coverage may be specifically excluded on the Computer Fraud insurance agreement. Also note that Funds Transfer Fraud insurance typically does not cover employee theft.

We'll be happy to help you analyze your need for and appropriate limits of Funds Transfer Fraud insurance as well as Computer Fraud insurance. Note that some insurers include fraud prevention education as well as discounts on security software along with their wrap policy.

We may be able to help you by providing referrals to consultants, and by providing guidance relative to insurance issues, and even to certain preventives, from construction observation through the development and application of sound human resources management policies and procedures. Please call on us for assistance. We're a member of the Professional Liability Agents Network (PLAN). We're here to help.