

May 15, 1998

Wire Transfers Invite Abuse

Security Procedures Can Protect Billions

A caller posing as a member of a large Southern bank's wire transfer department asked a clerk at an affiliated institution to verify the smaller bank's wire transfer identification number. The clerk who answered the telephone read off the number then became suspicious and called the large bank for confirmation. As a precaution, the upstream bank quickly invalidated the identification number. A short time later, someone tried to use the invalid number to transfer millions of dollars.

A customer established an account at two banks in different cities and began kiting checks into each account. After the balance in one accumulated to tens of thousands of dollars, he used a wire transfer to send the phantom money to the second bank, withdrew the funds and disappeared.

More and more companies—particularly financial institutions, brokerages, securities and investment firms—are using the electronic transfer of money for speed, anonymity, and—they think—security. In the last few years federal legislation and regulation have required financial institutions to report suspicious activity and adopt systems to help law enforcement track wire transfers. When the expanded format of Fedwire became fully implemented in 1998, passing information about the transactions to other institutions was no longer complicated for financial institutions. Operated by the U.S. Federal Reserve System, Fedwire is the nation's primary domestic electronic funds transfer system, handling both the message traffic started by financial transactions and the actual movement of funds. However, the very characteristics that make wire fund transfer systems attractive to business can leave them vulnerable to criminal abuse.

Wire Use Climbs

Electronic wire transfer systems move in excess of half a million transactions and approximately \$2 trillion around the world each day, according to the March 1996 report of the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN). The volume of wire transfers has increased substantially over the last 10 years and federal officials expect the volume trend to continue climbing.

With billions of dollars going over the wires daily, financial institutions and their clients are advised

to exercise caution when dealing with wire transfers. Wire transfer abuse such as fraud, check kiting or money laundering might not seem a significant problem—until customers and clients stop to realize that a single wire transfer transaction at a traditional financial institution averages in the hundreds of thousands of dollars.

In the Suspicious Activity Reports (SAR)—a report to FinCEN legally required of financial institutions—filed from April 1, 1997, to March 31, 1998, wire transfer fraud was suspected on 1,120 out of the 155,490 forms submitted nationally. An additional 371 suspected criminal cases mentioned wire fraud in the narrative section of the report when discussing other suspected problems, and 20 incidents probably involved wire fraud but were not recorded correctly on the SAR.

Federal officials say that criminal activity in the transfer of funds is often part of the case when such charges as loan fraud, check fraud or money laundering are filed. For example, a computer hacker gained unauthorized access to a large Eastern bank's cash management system, then used legitimate wire transfer procedures and accounts to transfer \$10 million out of the bank.

Incidents of wire transfer fraud are rarely reported publicly and those in financial institutions are reluctant to talk about them, even among themselves. "It goes to integrity—can I trust you with my money?" said one Chicago banker.

The \$70 Million Fraud

The most well-known case of wire transfer fraud—and the incident that led to tightening wire room security in the financial industry—involved a Midwestern bank in 1988. Two low-level employees provided secret codes and account numbers to another man who transferred nearly \$70 million from corporate accounts to banks in Austria. In one case the criminals impersonated the voices of two client executives who were authorized to transfer

(continued on next page)

Wire Transfers Invite Abuse

Security Procedures Can Protect Billions

(continued from preceding page)

funds from company accounts. The fraud was discovered when one of the victimized corporations noticed a substantial discrepancy in its account.

Two of the most common forms of wire transfer abuse reported on most recent SAR forms involve check kiting and false identifications, according to FinCEN officials. Check kiting is a systematic depositing of non-sufficient fund checks between two or more banks. Kiting is accomplished by taking advantage of the time it takes for a check deposited in one bank to be physically presented for payment at the bank on which it was drawn. The records of those banks show inflated balances that permit these checks to be honored. Wire transfers, which are guaranteed payments, are used to gain access to actual cash quickly.

Not as common as kiting, but still troublesome and getting more so, are incidents reported on SAR forms in which criminals obtain personal information about a customer and use this information to gain access to accounts. Money obtained from impersonating the customer is then wired to the criminal's bank and collected immediately, FinCEN officials report.

Businesses Lack Wire Transfer Security

Given the lax security of some of her clients, one banker said she is surprised there are not more incidents of fraud. "I have gone into some offices where the authorization code is taped to computer terminals," she said.

Businesses that have computerized codes or authorization numbers should have security controls in place to protect this information. Among the measures suggested by financial experts are: requiring two persons to access the codes, changing codes frequently, maintaining a random pattern of authorization code selection and requiring two separate codes to authorize a transfer order.

Some companies, one banker said, are willing to sacrifice some security for volume and speed when

they by-pass verification call-backs by the financial institution. They want the transfer executed before the bank or financial institution can call the home offices to verify the transfer. Often they write instructions allowing certain employees to authorize transfers up to a certain limit by voice. If the transfer is over the allotted amount, the financial institution must call the company bank and obtain a verification order from a second person.

By adopting a limited authorization policy, corporations are saying they are willing to risk a loss of up to a certain dollar limit to gain speed and convenience. Security directors for such firms develop ways to monitor the volume of transfers made under the authorization limit and any changes in an employee's lifestyle. In firms that allow such transfers by employees, security must include strict employee screening procedures.

Businesses that transfer funds to the same bank or company often will find using repetitive wires add both convenience—and an additional layer security. Repetitive wires act like a redial button on a telephone, except the person placing the order for the repetitive wire must have two separate codes.

Repetitive wires can be set up for a business by a bank or financial institution upon written instructions. The wire is set up to automatically send the amount desired to the designated party written in the instructions when authorized by a company employee who has both codes. In some banks the initiator of a transfer can be verified by a voice ID system and a password before a transfer is acceptable. The account number, amount of transfer, the name of the receiving party and other information is confirmed by the bank to prevent error.

The repetitive wire reduces the opportunity for clerical errors as well as criminal activity. Security directors for companies that use repetitive wires should make certain these numbers are kept in protected locations. In these cases security should also involve a list of employees who have access to the codes and when codes are used.

Screening and monitoring of all employees with access to codes are an important part of wire transfer security.

Checklist of Controls for Security Directors

Security directors should be alert to activities that may indicate wire transfer abuse. The U.S. Federal Reserve Board, the Federal Bureau of Investigation and the Comptroller of the Currency suggest looking for these signs of wire transfer fraud and other abuses, such as money laundering and check kiting:

- Indications of frequent overrides of established approval authority and other internal security measures;
- Intentional circumvention of approval authority by splitting transactions. Often funds will be deposited into several accounts in amounts below a reportable threshold, then consolidated into a master account;
- Frequent or large wire transfers for persons who have no account relationship with the institution;
- In a linked financing situation, a borrower's request for immediate wire transfer of loan proceeds to one of the banks where the funds for the brokered deposit originated;
- Large or frequent wire transfers against uncollected funds;
- Wire transfers involving cash where the amount exceeds \$10,000;
- Inadequate control of password access;
- Customer complaints and/or frequent error conditions;
- Frequent transfers of funds to and from off-shore banks or countries known as havens for their bank secrecy;
- An account or loan to be set up using a financial statement that reflects major investments

in and incoming funds from businesses incorporated in bank secrecy haven countries;

- Same check signature and payee, many out-of-area checks, escalating balances, frequent transactions, and money that stays a short time in the account can be signs of kiting.

Creating a Secure Wire System

Protecting the electronic transfer of funds begins with employees. Many experts believe that most workplace crimes such as wire transfer fraud are committed by ordinary people with incentive and opportunity.

Opportunity alert. Among the factors listed as opportunities that could alert security directors to the potential for employee crime are: weak or no internal audit committees; disciplinary actions that are weak or unpublicized and therefore not valuable deterrents; and non-existent or weak internal controls.

Hiring concerns. Companies concerned about employee crime in such sensitive areas as wire transfer operations should be prudent with employment practices. Careful employee background checks should include: criminal records, credit, work and professional history. Employers hiring employees for sensitive jobs should require: drug testing, polygraph testing where legally permitted, and psychological screening as part of the hiring process.

Danger signs. After employment, companies must be alert to changes in an employee's life or attitude about the workplace. Employee security revolves around knowing the people who are involved in the business. As one banker said: "Just because an employee has been with you 15 years doesn't mean you should trust him or her completely. Stay on guard."

Security directors should be alert to three danger signs as listed by the U.S. Treasury Department:

(continued on next page)

Wire Transfers Invite Abuse

Security Procedures Can Protect Billions

(continued from preceding page)

an employee whose lifestyle cannot be supported by his or her salary; an employee who is reluctant to take a vacation; and an employee who is associated with mysterious disappearances or unexplained shortages of significant amounts of funds.

Education needed. In some cases employees are not sufficiently trained in security procedures. For example, a staff security education program for employees might have prevented the loss of \$40,000 to one bank. A customer strolled into the branch office of a Southern bank and told a teller he had come to pick up a wire transfer that paid on proper identification. He gave a name—but no identification—and the teller handed over the money. The man and the money disappeared.

Pay attention. Often, simple details in training or awareness can reap large benefits. Using a common-sense approach to unusual requests or actions could prevent a crime or mistake. A frequent error in wire transfers occurs when client employees do not pay attention when the wire transfer order is read back to them. Employees should be trained to listen carefully and to make certain the customer on the other end of the telephone line listens carefully as well.

Carrying Security Further

A FinCEN official said that, trite as it may be, knowing customers goes to the heart of preventing wire transfer abuse. Knowledge of the customer and his or her business is another way to foil those who obtain personal information about clients, then use it to access accounts and wire money out of the account. A security director who understands the clients of his or her firm will recognize when a client's account shows out-of-the-ordinary transactions.

Today some institutions have computer software similar to that used by credit card companies that profiles customers. If a regular customer wishes to transfer funds to an unusual location or different party, the computer sends a warning signal.

While security directors are adopting measures to control wire transfer abuse on the local level, the Treasury Department and law enforcement agencies are developing new methods of making wire transfer unattractive to criminals. For example the new Fedwire format will make it easy for financial institutions and law enforcement to track wire transfers from destination to destination. Each wire transfer will now leave a trail that law enforcement can follow. And Treasury officials are working with 26 other nations in the Financial Action Task Force (FATF) to combat global money laundering and other forms of wire transfer abuse, most notably in the growing non-bank financial institutions transfer of funds.

Traditional financial institutions have led the way in preventing and detecting wire transfer abuse. These firms are big stakeholders in the wire transfer market—one mistake could mean huge losses. The latest federal regulations requiring transfer information and methods of tracking transfers are vital in the effort to stem the multi-million-dollar money-laundering operations of criminal activities around the world.

The security of wire transfers in traditional financial institutions and their business clients is based on precautions that should be part of every security director's policy and procedure manual. FinCEN at (703) 905-3770 is willing to provide information. Authorization codes and numbers, voice identification systems, and the security operation itself ought to be regulated closely—establish procedures and be certain they are followed.

However, it is the simplest rule of all that provides the greatest security: know your employees and your customers. If you do, you are more likely to spot a deviation in behavior that could signal wire transfer abuse.



The Lipman Report Editors