WIRE TRANSFER FRAUD

Hidden Dangers in Every Transaction

Lowers Risk Group – Risk Mitigation White Paper Series

LowersRiskGroup™
Protecting People, Brands, and Profits

(540) 338-7151 | www.lowersriskgroup.com

WIRE TRANSFER FRAUD

BACKGROUND

Approximately $2 trillion to $3 trillion moves around the globe daily over electronic funds transfer (EFT) networks. Much of this is done through point-to-point telecommunications links or the Internet. With so much money being transmitted in national and international commerce, it's inevitable that such transactions would be the target of fraud and theft. And almost all targeting that has succeeded has occurred at the hands of employees or contractors in a position of trust who have access to legitimate means to effect wire transfers.

Because of the potential for major losses, most corporations have stringent controls over every aspect of the wire transfer process, beginning with setting up repetitive wire transfers under dual control to daily reconciliation of all transactions by an independent person. However, some corporations do not always follow such rigorous procedures. Instead, they grant excessive authority to certain individuals, such as their Treasury Manager, to set up and initiate wires and then allow that same individual to reconcile the transactions. In other organizations, adequate controls are part of the corporate policies, but they aren't consistently followed. Failure to utilize or enforce proper controls is a recipe for disaster.

DEFINITION OF TERMS

To begin the review of wire transfer fraud, it is important to understand two distinct types of wire transfers:

1. *Repetitive Wire Transfers*: Repetitive wire transfers are used when funds are regularly moved between two specific accounts. Repetitive wire transfers consist of predefined information that requires the requestor to change only the dollar amount being sent. The initial data is entered once and the predefined data is given a repeat code so that it can be accessed on a repetitive basis without having to re-enter it.

   To set up repetitive wires, a person or persons authorized to set up wire transfer accounts may fax delivery instructions to the wire department of a financial institution. Or, the company's on-line cash management system may incorporate procedures whereby authorized individuals, with proper review, may establish repetitive wire transfers. In either case, the dollar amount of a repetitive wire may change each time one is initiated, but all other information must be constant.

Once established, the repetitive wires can also be automatically initiated and released for processing. The corporation determines the criteria for the transfer, including the amount, the debit and credit accounts, execution frequency (daily, weekly, biweekly, or monthly) and duration. From then on, funds are transferred as instructed until the standing order expires, or when the bank's wire transfer department is notified in writing of a change.

Fraud is rarely associated with repetitive wire transfers.

2. *Non-Repetitive Wire Transfers*: Non-Repetitive wire transfers are enacted on a one-time basis and require the corporate requester to complete all parts of the wire transfer request form.

TYPICAL /EXPECTED WIRE TRANSFER PROCESSES

The processes identified below apply to the corporate environment. They do not address internal controls that are specific to financial institutions.

1. Pre-employment Screening: The first "best practice" in the wire transfer process is to ensure that adequate pre-employment screening[1] and credit checks are conducted on all personnel assigned to the wire transfer function. Current employees should be re-screened if they are reassigned within the company to work in the wire transfer department. Re-screening should take place before the reassignment takes place and periodically.

2. Establishing Authorizations: The company should provide the bank with written instructions regarding the following:

   - If the bank is to initiate the transfers, then the bank should be provided with information regarding who is authorized to set up repetitive wire transfers, whose signatures should be on such requests, and what accounts can be involved. Signature cards should be on file for all such authorizations.

   - The bank should also be provided with the names of individuals who can authorize and verify non-repetitive wires, the dollar limitations on their authority, and the signature cards for each individual. Corporate wire transfer clerks should have a copy of these authorizations within their work area for reference.

   Even though the company might have an entirely computerized wire transfer request system, these authorizations should still be on file in the event the company's system malfunctions and

[1] "Adequate" pre-employment screening should, as a minimum, include criminal history record checks (felony & misdemeanor) in all jurisdictions in which the applicant has lived for the last seven years, credit check, drug screening, and all employment references checked for the last 7-10 years.

manual wire transaction requests must be processed. In addition, the wire transfer system user privileges, separation of duties, and authorization levels should mimic the manual environment.

3. Requesting/Authorizing Wire Transfers: Wire transfer requests could result from numerous requirements within a company, such as payments to vendors, processing of corporate payrolls, and investment activities by the Cash Management function. These three examples will be used to illustrate some of the differences in how transfers are initiated and processed:

   a. *Vendor Payments*: Wire transfer instructions for payment to a vendor should arrive from the Accounts Payable department with supporting documentation, such as the invoice, purchase order, shipping/receiving documentation, and possibly the contract. The appropriate individuals in accordance with the company policy should authenticate the instructions. Depending upon the dollar amount, a second person might be required to approve the instructions. These payments could be set up as repetitive wire transfers (such as in the case of a utility), or they could be non-repetitive wire transfers (such as payment to a consulting firm).

   b. *Payroll Payments*: Regardless of whether the company's payroll is processed in-house or by a payroll service, the supporting documentation for the amount of the payroll should be provided along with the wire transfer instructions. Normally, these wire transfers are repetitive wire transfers and the accounts to be debited and credited are pre-defined.

   c. *Cash Management Transfers:* A company's Cash Manager is normally a person specifically designated to manage the company's cash accounts. In some cases, the company's Treasurer or CFO performs this function. In other cases, a separate position is created to handle these activities.

      One of the activities typically performed by the person responsible is to make daily investments of the company's excess cash. To do this, the cash manager must move all excess cash from designated accounts to an investment account. Some companies automate this procedure and conduct an automated "sweep" of designated accounts and all cash over a specified limit is moved via wire to the investment account. Other companies will require that each movement of funds be documented via standard wire transfer procedures.

      Normally, the Cash Manager makes a determination as to what happens with the funds in an investment account and can direct such actions as: add to a Certificate of Deposit, authorize an overnight loan at current "Fed Funds" rates, purchase stocks or bonds, etc. These actions would normally be handled through an outside investment firm or a subsidiary of the company. Such actions would be taken by the investment agency based upon the

written/faxed/e-mailed instructions from the Cash Manager so that there is an audit trail of all actions.

4. Processing Wire Transfer Requests: Electronic funds transfers typically take place in the Corporate Finance Department.

   a. Manual systems: The actual wire funds transfer request that is sent to the financial institution is typically prepared by an administrative person and sent, along with the supporting documentation, to the first approving official for signature. Normally, repetitive wire transfers do not require a second approving official. For non-repetitive wires, the amount of the wire will usually determine whether a second signature is required. The approved wire transfer request is normally faxed to the company's financial institution (FI) or entered into the FI's cash management system. However, some smaller financial institutions will allow wire requests to be received over the telephone. Usually such conversations are recorded. Whether received by fax, telephone, or system entry, the financial institution's wire department will normally call back to the company and verify the transaction with an authorized individual whose name they have on file. This must be a different person than the original authorizing individual.

   b. Automated systems: The most common types of automated systems are described below.

      - *TYPE 1:* Company in-house leased application operating on bank-owned terminals and operating over leased telephone lines with a dial-up modem. As web-based systems have gained dominance, this type of system is rare.

      - *TYPE 2:* Web-based cash management application operated by the financial institution or a third-party application service provider on behalf of one or more financial institutions.

      - *TYPE 3*: Company in-house PC based application that interfaces with the bank's corporate cash management system over a leased point-to-point link or via an Internet/Web-based service. This system type is generally found to have more security problems than the other two types because of poor internal controls by the company.

      - *Repetitive Wire Transfers*: As an automated system, these wires can be designed to transmit automatically to the financial institution. They are formatted and completed in advance with all information pertaining to the payee, routing information, amount of payment, accounts to be debited and credited, and payment cycle dates. Or, if amounts differ each payment period, the company representative will be required to enter the amount before transmitting, but that is the only field on the template that can be modified.

- *Non-Repetitive Wire Transfers*: This type of wire requires all data pertaining to the wire to be entered by an authorized user based upon approved wire transfer instructions. Controls vary by companies at this stage. However, the better systems require one authorized user to prepare the wire transfer in the system and a second authorized user to verify and approve the release of the wire (also known as "data entry/verification entry"). The approving official should have the wire transfer instructions in hand when verifying the transfer. The approving official normally has read-only authorization and cannot change any of the data. Depending upon the controls in the system, the required approval/release authority can vary based upon the dollar amount of the wire.

5. Authenticating Users

   a. Manual systems: User name and password + callback. Callback and authentication are conducted over telephones and in plain text. This system is highly susceptible to compromise.

   b. Automated systems: System restrictions, application access rights, application privilege hierarchies, plus user name and password authenticated by the system. Some systems also utilize software or hardware tokens or biometrics, such as fingerprints, for "multi-factor authentication." Authentication security is dependent upon the security built into the application programs.

6. Transmitting the Wire Transfer Request to the Bank

   a. Manual systems: Typically, standard fax machines are used, despite their susceptibility to have their transmissions intercepted or faxes to be sent to the wrong number. While fax machines are available that have encrypting capability, they are rarely used.

   b. Automated systems

      - Type 1: Transmissions may or may not be encrypted during transmission. Encryption is NOT the standard.

      - Type 2: 128- to 256-bit encryption is the standard for these applications.

      - Type 3: Transmissions are usually encrypted, but the strength of the encryption may vary from 56-bit (low security) to 256-bit (high security) key lengths.

7. Physical Security Measures

   a. Manual systems: Little or no physical security is associated with manual wire transfer systems. The fax machine might be dedicated to the wire transfer function and

preprogrammed with the numbers of the appropriate financial institutions, but usually that is the extent of the physical security.

b. Automated systems

- Type 1: Though rarely used any longer, these are typically dedicated terminals with no other applications available for use. The terminals have internal IDs and the bank will not accept a transmission from any unauthorized terminal. These are usually located in isolated areas of the finance department. However, it is not normal to find them in secure rooms with good access controls.

- Type 2 and 3: The applications (including web browsers and specific client applications) are typically installed on selected PCs within the finance department, but no other physical security measures are normally taken.

8. Transmitting the Wire Transfer by the Bank: The financial institution's wire department encrypts the wire transfer instructions and incorporates a message authentication code (MAC). The wire transfer instructions are then sent over a leased line to the recipient's bank via Fedwire, CHIPS, or SWIFT.

9. Reconciliation: In order for adequate reconciliation to occur, the company must ensure the following documentation is in place:

- Source documents
- Wire service activity reports
- General ledger postings
- Automated control totals
- Transaction control sheets that include a unique message reference number, date & time of input, by whom input verified/authorized, date & time of transmission, accepted/rejected, and details of contents.
- Accepted/rejected message log. Reconciliation should occur no later than the following business day, with same day reconciliation preferred.

ESSENTIAL CONTROLS

1. Wire transfer policies and procedures have been incorporated into a written document; the document is current and contains all essential control elements contained herein.

2. Signature requirements have been established for all wire transfers as well as levels of authority for all authors and approvers of wire transfer requests.

3. Manual Systems and Backup to Automated Systems. Written instructions to the company's financial institution have been provided regarding account set-up and user authentication.[2]

4. For manual systems, stringent procedures are utilized by the company's bank to authenticate wire transfer requests.[3]

5. For automated systems, adequate procedures are utilized to authenticate users. These include the following:

   - Software or hardware tokens for terminal access[4]
   - Password controls for terminal and application access[5]
   - Additional user restrictions where technically feasible[6]

6. An audit trail is maintained of user access[7].

7. Entry and verification functions are appropriately segregated[8].

8. Wire transfer requests generated by the company through computer application programs are properly protected during transmission to the bank.[9]

---

[2] These procedures should include (I) Who can set-up accounts used in wire transfer processes (2) Who can establish repetitive wire transfers (3) Who is authorized to sign written/faxed wire transfer requests and what their level of authority. The instructions should include the provision that full signatures must always be used by anyone authorizing a wire transfer.

[3] As a minimum, these procedures should include the following: (1) Call-back procedures to predesignated individuals (2) Signature cards or signature lists for company personnel (3) Frequently changed customer identification numbers (4) Personal identification numbers and code words (5) Transaction reference numbers (6) Recording of all telephonic contacts with the wire transfer department of the financial institution.

[4] Biometrics (fingerprint, retinal scan, etc) are preferred above software and hardware tokens if available.

[5] Password controls should include the following: (1) Forced changes at least every 90 days (2) Must contain at least 8 characters and must use alpha, numeric, and special characters; (3) No repeating contiguous characters (4) No re-use of passwords (5) Minimum length of time between password changes is 7 days.

[6] If technically feasible, users should be further restricted by terminal ID, time of day, and day of week.

[7] The audit trail should contain a permanent record of (1) User ID (2) Date & time session began and ended (3) Transaction reference number (4) Any attempts at unauthorized log-on or attempts to work outside specific authorizations.

[8] (1) Entry & verification functions cannot be performed by the same individual (2) Entry & verification functions cannot be performed from the same terminal (3) Verification positions are prohibited by the application from correcting, changing, or deleting any data.

[9] Technical measures such as Secure Socket Layer (SSL), Virtual Private Networks (VPN), and digital certificates and digital signatures are employed. 128-bit encryption, as a minimum, is used during these processes

9. The company receives advice statements daily from the bank on wire transfers to and from accounts; these statements are used to conduct settlement and reconciliation at least once per day.[10]

COMMON VULNERABILITIES

1. Pre-employment screening is:
    - Inadequate from the start, and/or;
    - Re-screening is not conducted upon re-assignment to wire transfer duties, and/or;
    - Periodic re-screening is not conducted of individuals after they are assigned to perform wire transfer duties.
2. Companies utilize non-secure faxes and non-secure connections for transmitting wire transfer requests and for authenticating transactions using callback procedures.
3. User authentication is weak.[11]
4. Internal controls over the process of preparing wire transfer instructions and supporting documentation are weak.[12]
5. Initials are allowed to be used to authorize and/or approve wire transfers instead of full signatures.
6. Senior managers involved in the cash management function have excessive rights and privileges, i.e.,
    - They can assign users to the wire transfer system and establish their rights and privileges.
    - The cash manager can create templates for repetitive wires with all transfer instructions built in.

[10] The person conducting the reconciliation should not be involved in the authorization or approval of wire transfers. If access to the wire transfer program is required for reconciliation, it should be on a "read-only" basis. Normally, there is a cut-off time by the bank for daily wires by mid-afternoon. Reports from on-line systems are usually available within 1-2 hours after the bank's cut-off time. This should allow all daily wires to be reconciled by the company the same day they are processed, or at the latest, the next morning.

[11] Under the Uniform Commercial Code, Article 4A, simply requiring passwords "cannot constitute commercially reasonable security." And the banks cannot be held responsible for an erroneous or fraudulent wire transfer unless the company can PROVE that the perpetrator of the fraud was not an employee or former employee or agent or former agent of the company. Therefore, strong user authentication is critical to avoid liability.

[12] Some companies allow senior managers to verbally direct that a wire transfer take place and that the manager will follow-up with written instructions later. Other companies do not require dual control on any wire transfer instruction, approval, or authorization.

- The cash manager has the authority (single control) to create bank accounts at the financial institution for use in the wire transfer process.
- The cash manager can transfer funds between wire transfer accounts under single control (authorize and approve).
- Senior managers are involved in the reconciliation process as well as the wire transfer authorization and approval process.

7. Reconciliation is not performed on a timely basis.

COMPENSATORY MEASURES

1. Strengthen screening and re-screening employment practices.
2. Where systems or processes are found to have vulnerabilities that can be exploited by a sole individual, integrate dual controls immediately into all processes involving preparation of wire transfer instructions, and authorizing and approving such transfers.
3. Ensure there is independent and frequent review of investment transactions by a knowledgeable party.
4. Conduct semi-annual audits of the wire transfer function. Ensure auditors review password requirements and controls during each examination.
5. Conduct annual penetration tests and annual security audits of web-based wire transfer applications that are hosted by the company or by a third party application service provider.

CASE STUDY #1

A start-up Internet banking service revealed a flawed security policy that allowed customers to transfer funds without verifying bank account numbers resulting in close to $10,000 worth of illegal transfers. But at least one person charged that online thieves tried to transfer more than $50,000 from his bank account using a stolen account number. Before revising its policy on Jan. 22, X.com Corp. in Palo Alto, Calif., allowed customers to transfer up to $2,500, from any U.S. bank account and then withdraw the money by entering only the account and bank routing numbers on the X.com Web site.

According to company CEO William Harris, the would-be crooks, entering data from customer's accounts, attempted six unauthorized fund transfers that were halted by X.com. Imad Khalidi, CEO of Auto Europe LLC, a car rental agency in Portland, Maine, said he discovered on Jan. 14 that someone had used his account number to siphon $21,000 out of his company's bank account to pay for Gucci merchandise. Khalidi said thieves made four other attempts to transfer money from his account via X.com and Wilmington, DE-based WingspanBank.com, including an attempted $23,000 transfer. The online grifters then posted Khalidi's account numbers to an Internet forum.

According to Harris, X.com has changed its security policies to require customers to fax or mail a voided check, signature card, and a copy of a driver's license to verify bank account numbers for transfers of any value.

CASE STUDY #2

One large corporation that used EFT extensively would routinely deliver a magnetic tape loaded with multiple wire instructions every day. The company was supposed to apply a unique identifier to the tape box, and the bank was supposed to inspect it to make sure the tape was authentic, but the procedure became so routine that the tape authentication drill was relaxed.

That mistake almost proved fatal when an insider slipped a bogus wire instruction onto a bogus tape and the bank accepted and executed the tape, including a bogus wire directing a large amount of money to a private offshore bank account. An alert banker, up the chain from the bank where the wire was initiated, caught it just before the funds would have left the country.

CASE STUDY #3

In another incident several years ago, wire instructions were authenticated by callback. Someone in the bank's wire room would pick up the phone and call the authorized corporate official to confirm that a wire request the bank received was indeed authentic. Culprits inside the company

used automatic call forwarding to bypass the real authority and divert the calls to someone who was in on the scheme and would approve the fraudulent wires. Once again, it got past the initial bank and was caught further up the line before the funds left the country.

CASE STUDY #4

Another near-loss was perpetrated by a consultant who had been working in a large bank for months and had stolen the internal codes used by bank personnel to authorize wires. He also had found out which accounts had high balances and almost no activity. One day he called the bank's wire room, gave the proper code to identify himself as a branch officer of the bank, and directed $10 million to his own Swiss bank account. The transfer took place. The man even withdrew some of the money to buy several diamonds. But the theft was detected, the man was arrested before he could leave the country, and nearly all of the money was recovered.

GLOSSARY OF TERMS

Automated Clearinghouse: The ACH (Automated Clearinghouse) Network is a nationwide electronic payments system used by more than 15,000 participating financial institutions, 40,000 corporations, and millions of consumers. This service allows participating entities to write checks, and make deposits electronically. The most basic and widely used type of ACH transaction is direct deposit. Payroll, dividends, interest, annuities, employee expense reimbursements, pensions, and investment income are some of the more important direct deposit transactions.

CHIPS (Clearing House Inter-Bank Payments System): CHIPS is a bank-owned, privately operated real-time, final payments system for business-to-business transactions in the United States. Their web page advertises the following services:

- The premier U.S. dollar payments system
- Electronic Data Interchange (EDI) - remittance information arrives with the payment expediting reconcilement
- Real-time settlement of transactions
- Alternative to Fedwire for business-to-business payments

Most CHIPS transfers result from international transactions. CHIPS transfers are settled on a net basis at the end of the day, using Fedwire funds transfers to and from a special settlement account on the books of the New York Fed.

EDI (Electronic Data Interchange): The inter-company electronic transmission of business documents in standard formats.

EFT: Electronic Funds Transfer

Fedwire: The Fedwire funds transfer system is a real-time gross settlement system in which more than 9,000 depository institutions initiate funds transfers that are immediate, final, and irrevocable when processed. Depository institutions that maintain a reserve or clearing account with a Federal Reserve Bank may use Fedwire to send payments to, or receive payments from, other account holders directly. Depository institutions use Fedwire to handle large-value, time-critical payments, such as payments for the settlement of interbank purchases and sales of federal funds; the purchase, sale, and financing of securities transactions; the disbursement or repayment of loans; and the settlement of real estate transactions.

In the Fedwire funds transfer system, only the originating financial institution can remove funds from its Federal Reserve account. Originators provide payment instructions to the Federal Reserve either on line or off line. On-line participants send instructions through either a mainframe or PC connection to Fedwire.

Flat text file: Flat text files (or import files) are ASCII text files containing one record per line, with each line terminated by a carriage return and line feed.

MAC (Message Authentication Code): A specific type of message digest where the secret key is included as part of the message fingerprint or 'hash.' Hash functions are well suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence.

Non-Repetitive Wire Transfer: Completed on a one-time basis and requires the corporate requester to complete all parts of the wire transfer request form. Repetitive wire transfers are used when funds are regularly moved between two specific accounts. Repetitive wire transfers consist of predefined information that requires the requestor to change only the dollar amount being sent. The initial data is entered once and the predefined data is given a repeat code so that it can be accessed on a repetitive basis without having to re-enter it.

SWIFT (Society for Worldwide Inter-bank Financial Telecommunication): SWIFT was formed when seven major international banks met in 1974 to discuss the limitations of Telex as a means of secure delivery of payment and confirmation information, primarily in the Treasury and Correspondent banking areas. The decision was taken at that time to form the society and three years later in 1977, 230 banks in 5 countries went live. New countries and users are added four times a year with recent figures showing over 184 countries and 6700 institutions connected. Uniquely, SWIFT takes full liability for each message once they have accepted it, and it is probably this linked to the inbuilt security and robustness of the network (consistently better than 99.99% up time every year) that has led to SWIFT's dominant position in the market. Although originally the network was designed to support the requirements of Treasury and Correspondent banking operations, it has over the years allowed other institutions access to the services, albeit in some cases only to a limited degree. Currently the following categories of organization can access the service:

- Banks
- Trading Institutions
- Money Brokers
- Securities Broker Dealers
- Investment Management Institutions
- Clearing Systems and Central Depositories
- Recognized Exchanges
- Trust and Fiduciary Service Companies
- Subsidiary Providers of Custody and Nominees
- Treasury Counterparties
- Treasury ETC Service Providers

LOWERS RISK GROUP – Fidelity & Crime White Papers

There are three conditions that are present when fraud occurs: Opportunity, Incentive, and Rationalization. The information contained in these papers demonstrates examples of vulnerabilities and how applying essential controls can significantly reduce the risk of fraud.

ABOUT LOWERS RISK GROUP

Lowers Risk Group combines the services of three industry-leading companies – Lowers & Associates, Proforma Screening Solutions, and Wholesale Screening Solutions – to create a complete risk management service offering for organizations of all shapes and sizes. Employed in concert or on a standalone basis, we excel in providing comprehensive enterprise risk management and human capital risk solutions to organizations operating in high-risk, highly-regulated environments. Our specialized background screening and crime and fidelity risk mitigation services protect people, brands, and profits from avoidable loss and harm. With Lowers Risk Group you can expect an experienced and professional approach to your risk assessment, compliance, human capital, and risk mitigation needs to help move your organization forward with confidence.

Contact Information:

Lowers Risk Group
125 East Hirst Road
Suite 3C
Purcellville, VA 2 0132

Telephone: 540-338-7151
Fax: 540-338-3131
Email: info@lowersrisk.com
Web: www. lowersrisk.com