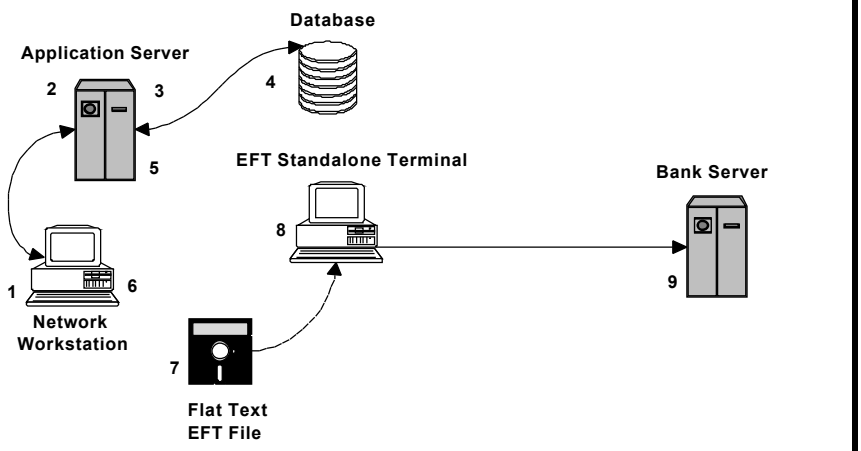
Global Information Assurance Certification Paper

INTRODUCTION

Before defining the steps for preventing electronic funds transfer (EFT) fraud, it is necessary to define EFT and common motivations of individuals who commit EFT fraud.

The EFT process is the means by which an organization transmits payment instructions to a financial institution for imbursement of employees, third parties and/or other entities. Although numerous technical solutions exist, this paper addresses a frequently deployed solution, which involves components and steps cited in *Exhibit 1*.



1 - Authorized company employee uses network workstation to request creation of an EFT file;
2 - Request is received and processed by application server;
3 - Application server queries database for EFT data;
4 - EFT data is extracted from database and used to generate a flat text EFT file;
5 - EFT file is saved to a secure directory located on the application server;
6 - Autorized company employee copies EFT file to diskette residing in network workstation;
7 - Authorized company employee inserts diskette into standalone EFT terminal for transmission;
8 - EFT file is transmitted to bank as an encrypted flat text file; and
9 - Bank processes EFT file.

EXHIBIT 1

The motives behind EFT fraud are vast and complex. Common motivating factors include significant financial gain, desire to master the EFT system, thrill of the deed, and employee revenge.

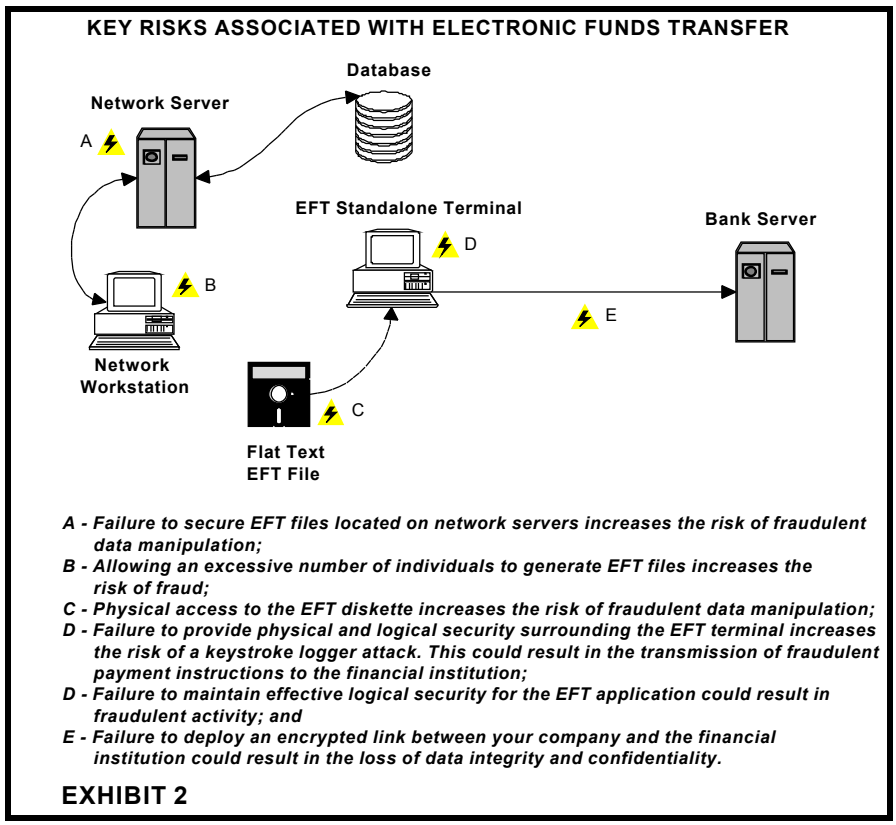
Often, very large dollar amounts are transmitted over EFT networks during a single EFT transmission. By fraudulently altering payment instructions in the EFT process, an individual could potentially steal large sums of money. Although it is difficult, if not impossible, to obtain accurate statistics on EFT fraud, one could suggest that millions of dollars are loss by companies per year to fraudulent EFT payment instructions. In order to avoid embarrassment and a potential decline in share price, most companies prefer not to release information pertaining to fraudulent activity to the public.

Hackers commonly penetrate systems as a recreational activity. When asked about their reasons for compromising a computer or introducing a virus on the Internet, hackers commonly state that their intentions were not to cause harm but "to see whether they could actually do it." Similarly, those who commit EFT fraud may merely want to determine whether they can perfect the EFT system and/or process. EFT crime offers an intellectual challenge, which is as attractive to some as the opportunity for financial gain. [1]

In today's corporate world, mergers, acquisitions, and streamlining of business processes are common occurrences. Positions sometimes become redundant, and employees consequently lose their jobs and livelihood. Such an environment increases the risk of EFT fraud. An employee at the EFT controls could anticipate a loss of employment and retaliate against the company by releasing a fraudulent EFT payment to their own bank account.

STEPS FOR PREVENTION

In order to reduce the risk of fraud, several controls can be incorporated into the EFT processing environment. The integration of these preventive steps into the process will reduce the risk of EFT fraud. However, these steps should not be considered a "silver bullet", which will spoil all fraud efforts.



Define the EFT Process and Control Points

An important first step is to gain an understanding of the EFT solution and process.

To facilitate this understanding, a useful exercise entails defining the EFT process and procedures used to transmit EFT files to the financial institution. During this process, it is also useful to identify risks, vulnerabilities and control points. Technical specifications often provide an excellent starting point. If technical specifications are not available, it is helpful to conduct an informal workshop with all necessary employees whom you know are involved in the EFT process (e.g. Finance, Payroll, IT business representatives, etc.). Any employees involved in EFT manual and automated processes and supporting infrastructure should be consulted. Upon identification and definition of the EFT process, risks vulnerabilities and control points should be outlined. Refer to *Exhibit 2* for examples of key risks associated with the EFT process.

Define EFT Policies and Procedures

The real threat faced by finance managers is rather mundane, which includes how to keep their own staffs from ripping off the company. The solutions are similarly ordinary and include common sense policies and procedures pertaining to:

- Auditing regularly;
- Reconciling promptly;
- Screening employees carefully; and
- Requiring two approvals before funds can be transferred. [2]

In order to ensure consistency of EFT practices, it is important to establish formal procedures. All employees involved should be educated on the content of the procedures. In addition, it is necessary to establish an EFT policy, which defines acceptable practices and implications of non-compliance with the policy. Prior to participating in the EFT process, employees should be required to read and abide by the conditions stated in the policy. The criticality and integrity of the EFT process must be stressed in the policy.

Ensure Physical Security Surrounding All EFT Components

Physical security surrounding the EFT hardware and software components cannot be stressed enough. On occasion, I have conducted reviews of companies' EFT processes and noted entire solutions could be easily compromised because of an outright disregard for physical security. Frequently, companies install a financial institution's EFT software on a standalone workstation. If this workstation utilizes a NT 4.0 platform and lacks physical security, the potential of fraudulent activity increases. Following are steps, which could be used to easily compromise such a configuration:

1) Gain physical access to the EFT workstation;
2) Reboot the EFT workstation from diskette;
3) Download the NT Security Account Manager (SAM) database to diskette;
4) At a remote workstation, use l0phtCrack (a tool available on the Internet) to crack the SAM;
5) Return to the EFT workstation and login with an NT login ID, which was

cracked with l0phtCrack;
6) Install a keystroke logger program on the NT workstation, and subsequently use the logger to capture passwords used to authorize EFT file transmissions to the bank;
7) Send fraudulent EFT payment instructions to the bank; and
8) Leave the country for vacation.

As the example demonstrates, physical security is a key control surrounding the EFT process. If your EFT solution lacks physical security, the mentioned scenario should alarm you.

Implement Effective EFT Application Security

Too often, organizations wholeheartedly purchase and immediately implement a new application without understanding the security capabilities of the software. An emphasis is placed on installing the application into production as soon as possible. Similarly, EFT applications are sometimes placed in a production environment without the appropriate logical controls. Whilst EFT software packages support similar security capabilities, these applications also offer unique security configurations. Prior to implementation, an application security review should be conducted to determine the appropriate security parameters. In addition, user profiles should be designed to enforce segregation of duties amongst sensitive EFT functions (e.g. application IDs with the ability to transmit EFT files or create/delete user IDs) and the least privilege principle. *Exhibit 3* provides an example of a user profile matrix. The matrix demonstrates that any combination of users may be used in the creation, authorization, and transmission of files, provided that two separate authorizers are used. In the following examples, at least two users are required to complete the transaction. This example demonstrates the simplicity of generating secure EFT access profiles. Upon completing the access security review and

Create EFT	First Authorization	Second Authorization	Send EFT
User1	User 2	User 3	User 4
User1	User 2	User 3	User 1
User 1	User 1	User 2	User 2
User 1	User 1	User 2	User 1

EXHIBIT 3

[3]

designing user profiles, management endorsement should be obtained through sign-off. Although this may appear to be too official, the transmission of millions of dollars per year through an EFT application is a serious matter. Some key items to consider prior to implementation of an EFT application include:

- Minimize the number of application administrators;

- Change default password for administrator account;
- Maintain passwords to default application IDs in a secure location;
- Require dual authorization for the creation and deletion of users;
- Require dual authorization for the release of EFT files to the bank;
- Ensure timely maintenance of user accounts;
- Limit failed login attempts to the application;
- Require periodic password changes; and
- Limit dollar amounts of EFT transmissions (e.g. EFT file cannot transmit a payment amount exceeding $20,000,000).

Implement Effective Network Operating System Security

As mentioned earlier, physical security of an EFT workstation is crucial. If a workstation is physically accessible, the network operating system could serve as an avenue of attack. In addition, network operating system services and ports should be reviewed for appropriateness. This is commonly referred to as "hardening the operating system" and is similar to the application security review process. Services and ports not required within the operating system should be disabled to reduce the risk of unauthorized access to the workstation. Also, an additional key control entails disabling the floppy disk drive, so that the network operating system does not boot from diskette. [4] This prevents an individual from easily gaining unauthorized access to the EFT application. Following are additional controls and resources, which should be used to enhance network operating system security:

- Limit the number of network operating system users with access to the EFT workstation;
- Enable the screensaver timeout feature;
- Restrict remote access to the terminal through in-bound modem connections; and
- Utilize the SANS Institute's "Windows NT Security Step By Step" document as a guide for securing the network operating system.

Implement Effective Security Surrounding EFT Data

Ensuring integrity and confidentiality of data throughout the EFT process is critical. It is data-related crimes, which are the most common. [5] EFT crime is often difficult to detect because data can be manipulated by instructions hidden in complex computer software. [1] As *Exhibit 2* illustrates, EFT data can reside in multiple locations and must be logically secure at several layers (e.g. database, network operating system, diskette and transmission). Since EFT data is potentially subject to modification at the mentioned layers, automated and manual controls should be employed to minimize risk. For example, upon generation, an EFT file could be saved to a directory, which resides on a network server. Access surrounding the EFT file and directory should be restricted to prevent tampering with dollar amounts and/or bank account details. In addition, as *Exhibit 2* illustrates, the EFT process could involve saving data to diskette. Care should be given to physical security surrounding the diskette in order to decrease the risk of data modification. It is good practice to maintain the diskette under dual control until the EFT file is transmitted to the financial institution. I have observed

EFT processes, which have involved the use of the "Windows Notepad" program to make revisions to data. This practice is unacceptable and should be highly discouraged. Uncontrolled changes to data could result without a supporting audit trail. Finally, during transmission of the EFT file to the financial institution, data must be encrypted to ensure privacy and integrity. Encryption of EFT data can occur via hardware or software.

Implement Effective System Logging

Some dismiss the value of system logging and argue that it is a time-consuming process and wastes system and operational resources. However, most familiar with the importance of the EFT process would agree that the benefits of logging definitely outweigh the costs. Most importantly, logging establishes a baseline, which can be used to measure unusual activity. Specifically, logging allows one to capture unauthorized modification of EFT payment instructions and/or transmission of EFT files. Further, logging provides an audit trail, which could serve as evidence during legal proceedings.

When one considers the EFT architecture, it becomes evident that logging can occur at multiple levels. As *Exhibits 1 and 2* illustrate, several points exist within the process where data could be viewed and/or altered. This is an important reason for enabling logging and periodically monitoring activity. Following are some examples of activities, which could be logged during the EFT process:

- Generation of EFT files;
- "View" and "edit" access to the EFT file, which is saved to a network operating system directory and/or diskette;
- Changes to the database, which contains EFT data;
- Creation and deletion of EFT application user IDs; and
- EFT transmissions to financial institutions.

Upon defining the EFT architecture and process, it is relatively easy to determine where system logging should be enabled. A strategy should be defined, which considers the following topics:

- Components to be included in the logging process (e.g. EFT application and network operating system);
- System activity to be logged (e.g. generation of EFT file);
- Storage locations of system log files;
- Personnel responsible for monitoring system logs;
- Frequency of monitoring system logs;
- Interpretation of system logs;
- Examples of unusual activity noted in system logs;
- Procedures for handling unusual activity discovered in system logs; and
- Archiving and data retention of system logs and EFT reports.

Conduct Reconciliations

Similar to logging, reconciliations can occur at several points within the EFT process. Reconciliations are important and allow one to determine whether data has been modified during any stage of the EFT process. Upon generation of the EFT file, a record count (e.g. total transactions) and total dollar amount should be produced. This information can be used as source documentation for future reconciliations. Following transmission of the EFT file to the financial institution, an EFT report (e.g. transaction

report) should be downloaded from the financial institution. This report provides a record of total transactions and dollar amounts and can be used to compare source transactions and dollar amounts. Remember to save all documentation, which could be required for future reference. These documents serve as an audit trail and substantiate the reconciliation process. Further, as proof that the reconciliation actually occurred, the person responsible should initial documentation.

CONCLUSION

This paper commenced with a definition of EFT and common motivations of individuals who commit EFT fraud. Thereafter, steps for preventing EFT fraud were discussed. Although the mentioned steps will not absolutely prevent fraud, incorporation of these practices into your company's EFT solution will reduce the risk of EFT fraud occurring in your work environment.

Armoured cars with armed guards frequently deliver and retrieve cash from businesses. Security surrounding the delivery of physical money tends to be high. Conversely, occasionally, I visit companies who frequently transmit several millions of dollars in electronic form to financial institutions on a monthly basis. Some of these companies fail to incorporate basic physical and logical controls into their EFT processing environment. Consequently, anyone with an understanding of the EFT process and technical knowledge could easily transmit fraudulent payment instructions to a financial institution. Is your company susceptible to EFT fraud? Remember. Preventing electronic funds transfer fraud pays.

REFERENCES

[1] "Selected Electronic Funds Transfer Issues, Privacy, Security, and Equity." URL: http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk3/1982/8223/822303.PDF

[2] Gamble, Richard. "Short Circuiting Wire Transfer Fraud." Controller Magazine. August 1998. URL: http://www.businessfinancemag.com/archives/appfiles/Article.cfm?IssueID=325&ArticleID=4389

[3] "Guidelines for the Use of DeskBank." Department of Treasury and Finance. October 1999. URL: http://www.treasury.tas.gov.au/domino/dtf/dtf.nsf/acca8cad9e1c8f864a256807001974ce/b3bb3aa29bbb681c4a256818000b1f9d?OpenDocument

[4] Windows NT Security Step By Step, Version 2.15. The SANS Institute, July 30, 1999. Page 11.

[5] Ajinkya, Tushar and Ogoti, Annapoorna. "Weeding Out Risks in EFT Transactions." Business Line. May 19, 2000. URL: http://www.indiaserver.com/businessline/2000/05/19/stories/151939m3.htm