

Preventing EFT Fraud with Training Reducing Risk to Financial Institutions and Their Customers

By Dr. Linda Eagle

The growing popularity of Electronic Funds Transfers (EFTs) may soon make paper bills obsolete, as more individuals discover the ease of accessing their bank accounts and transferring money electronically each day. EFT services are quickly becoming one of the fastest growing segments of the financial services industry in the US and abroad. However, with this trend, an increasing number of frauds involving money laundering and identity theft in EFTs are continuing to emerge.

While affording convenience, EFTs put the customer at risk for serious security problems. In the US alone, an estimated \$500 billion is electronically transferred among financial institutions daily, providing criminals and financial terrorists vast opportunities to intercept funds.¹ To further complicate the problem, evidence suggests that credit risk and fraud are of even more concern during weak economic periods, when bankruptcies and business failures are more prevalent.

Therefore, it is imperative that financial institutions be fully aware of the dangers EFTs pose and the steps they must take in order to maintain the security of their funds, as well as the funds of their customers. In order to protect their customers against fraud, financial institutions must be proactive in their approach to training their staff on how to identify risks associated with EFTs.

What Is an EFT?

An EFT is the electronic exchange or transfer of money from one account to another, either within the same financial institution or across multiple institutions. In modern society, many of our banking activities are performed electronically. Whether a customer is withdrawing money from an ATM, using a credit card at a gas station, paying bills and buying products online or transferring money from an account to another through a financial institution's website, s/he is performing an EFT. EFTs can even be performed from a cell phone or Personal Digital Assistant (PDA). And there are often many steps. In the US, for example, before an EFT can be posted as either a debit or credit, it must first pass through an Automated Clearing House (ACH), a system of the US Federal Reserve Bank that provides EFTs between banks.

¹ Effy Oz, "EFT Risk Issues and Control Procedures," [http://findarticles.com/p/articles/mi_qa3682/is_199401/ai_n8717764/], March 19, 2010.

What Are the Risks?

Though the extent of services varies, typical electronic banking services include credit and debit cards, deposits, wire transfers, and bill-paying services. Electronic banking is vulnerable to money laundering and terrorist financing because of its user anonymity, rapid transaction speed, and its wide geographic availability. Customers who perform their banking through ATMs, online accounts, or through their PDAs are at risk and need to take a closer look at their account details on a regular basis.

Many customers do not understand how these systems operate and the many risks they are exposed to. Criminals have created highly sophisticated Trojan viruses (e.g. the Clampi virus) that steal online banking log-ins when customers sign on to their financial institution's websites, open an attachment in an email or click on certain links or pictures. Once on the computer, the virus may remain unnoticed until the user logs on to his/her online bank where it then captures the log-in and password information, and sends it to a server run by the attackers. Attackers are then able to wire cash transfers to "mule" accounts they control using banks' ACH systems. At this point the attackers can make online money transfers or they can buy goods with the stolen account details.

EFTs can be used at all stages of money laundering, which include the following areas.

- **Placement.** Placing illegally gained cash into a legitimate financial system or legitimate commercial entity.
- **Layering.** The process of separating the source of cash from its criminal origins by passing it through several transactions.
- **Integration.** Combining illegal funds with legally obtained funds in an effort to blur the makeup of the account.

The Impact of EFT Fraud on Businesses

EFTs are the most prevalent method that business customers and financial institutions use to transfer funds. Business customers of all financial institutions should be concerned over the safety of their accounts. Nearly 40 percent of business customers are unsure if EFT/AML programs even exist at their financial institutions.

According to recent research conducted by the Ponemon Institute and Guardian Analytics, 55 percent of small and medium businesses in the US were fraud victims in the last 12 months, with 58 percent of fraud enabled by online banking activities. Even more startling is the fact that 80 percent of financial institutions failed to catch the fraud before funds were transferred out. In 87 percent of fraud attacks, the financial institution was unable to fully recover assets and 57 percent of the victims were not fully compensated by their financial institution with 26 percent left uncompensated for any part of their loss.² This study illustrates just how large a problem money laundering and fraud have become in our internet based and fast moving modern society. With no end in sight to both consumer and financial institution dependency on the internet and electronic services, financial institutions and their customers need to be trained and aware of the steps they can take to secure their accounts.

² Penny Crossman, "Rise in Online Banking Fraud Costing Banks Customers, Study Says," [<http://www.banktech.com/riskmanagement/showArticle.jhtml;jsessionid=WEFVQFOR1ROYXQE1GHPCKHWATMY32JVN?articleID=22340002>], March 10, 2010.

Reducing Risk with Training

Both personal banking and business customers must be particularly cautious when using their online bank accounts, and must know which steps to take to prevent fraud. Many issues can be avoided by training employees on how to advise customers to complete simple actions to protect themselves against risk. Changing passwords frequently, using encryption, using strong anti-virus protection software, being cautious when opening emails and links and closely reviewing statements are all smart ways for customers to protect their financial resources.

Financial institutions offering EFT products and services to their customers need to have sound AML policies, procedures and processes in place to manage the risks associated with EFTs. Without these regulations, the risks of electronic banking can result in financial loss and reputation damage for the financial institution through fraud, disclosure of customer information or corruption of data. There are many warning signs of potential fraud that bank staff must be informed of and prepared for. At a minimum, financial institutions should evaluate the following:

- Customer types.
- Transactional capabilities and patterns.
- Methods of money transfer.
- Volume and number of transactions.
- Geographic location of originators and beneficiaries.

Financial institutions should report suspicious activities associated with EFTs to appropriate regulatory and law enforcement agencies. In the US this is required by the Bank Secrecy Act (BSA). The Act's AML requirements mandate that financial institutions keep records and file reports for certain types of transactions, such as EFTs, and establish programs to prevent and detect money laundering. By law, banks are required to report suspicious transactions using a Suspicious Transaction Report (STR). STRs must include certain information including the nature of the transaction and parties involved, as well as how the suspicious transaction was detected. STRs assist governments in criminal prosecution purposes by providing clues to the evolving patterns of money laundering schemes.

Final Word

As more bank customers begin to use electronic banking solutions, hackers and money launderers are becoming more creative in their fraud tactics. Simply put, EFTs are subject to high risk and exposure to fraudulent activities, and fraudulent activity is damaging to a financial institution's relationship with its customers. To counter this, financial institutions must proactively invest in AML training to better prepare their employees to identify the risks that may occur in ETF transactions, and to educate their customers on how to protect themselves from threats to the security of their funds. Specialized training from an accredited training provider should be considered by all management of financial institutions to manage the risks and meet demand as this banking trend continues to grow.



Dr. Linda Eagle is Founder & President of The Edcomm Group Banker's Academy—a 23-year-old education and consulting firm dedicated to serving Banks, Credit Unions, Money Services Businesses (MSBs) and all areas of the Global Financial Community with thousands of generic and customized training programs in areas such as BSA/AML, Regulatory Compliance, Teller Training, Systems Training, Sales and Service Training, and many more.

[The Edcomm Group Banker's Academy](#) is headquartered in New York, NY. For more information, email linda.eagle@edcomm.com or call +1.212.631.9400.