

EFT Fraud Prevention

By Derek Hammen, CPA



In an ever-emerging electronic age, more businesses are integrating the use of technology into their cash disbursement process through means of Electronic Funds Transfer (EFT) transactions – these include wire transfers and automated clearing house transactions – leaving them susceptible to cyber theft. Over the past year, there has resultantly been an increase in reported EFT fraud against small to medium-size businesses. Cybercriminals are able to gain remote control of a victim’s computer system, enabling them to withdraw funds as what appears to the bank’s security system as legitimate transactions. In most cases of EFT fraud, the victims will be unable to recover their funds or successfully sue the bank receiving the stolen funds.

According to recent research, 55% of small and medium businesses in the U.S. were fraud victims in the last 12 months, with 58% of fraud enabled by online banking activities. 80% of financial institutions failed to catch the fraud before funds were transferred out. In 87% of fraud attacks, the financial institution was unable to fully recover funds, 57% of the victims were not fully restored by their financial institution, and 26% of victims were left uncompensated for *any* part of their loss.¹ Considering these startling figures, we recommend anyone using electronic banking take steps to minimize exposure to loss.

Although financial institutions have security measures in place, there are preventative and detective procedures businesses can implement on their own. In order for businesses to protect themselves from the damages this type of fraud can cause, we recommend implementation of a combination of the following to mitigate the associated risk:

- Dedicate a computer or system specifically for online banking
- Use a multifactor authentication with an independent mechanism
- Segregate EFT controls
- Dedicate clearing accounts using “just-in-time” deposits
- Reconcile EFT transactions daily



Dedicated computers or systems should be used strictly for conducting EFT transactions and should not be used for e-mail, web browsing, or any other activity that could condone malicious attacks from cybercriminals. This limits the likelihood of a cybercriminal breaching the computer’s system.

¹ Ponemon Institute and Guardian Analytics, 2010

Some banks offer a security feature that uses a “**multifactor authentication**” with an independent device (e.g. keyfob or pager). This method delivers a one-time password or PIN to the independent device that is used to login into financial accounts, making it nearly impossible for a cybercriminal to gain access since the device is not at all a part of the computer or online system.

Segregating EFT controls places emphasis on dual-control processing: have one person initiate the EFT transaction that is then automatically forwarded to another person approving them, which is finally systematically forwarded to the bank. If a business’ computer system cannot support this process, their bank may provide a similar type of segregation control or the business can perform this measure manually.

Establishing a clearing account to perform all EFT transactions is a best practice for a practical way to combat fraud. An entity would block all of their bank accounts from withdrawing funds through EFT transactions except for one account, which would carry a zero balance. The entity would then deposit enough funds into the clearing account to carry out any EFT transactions just-in-time; thus, limiting the exposure of significant cash balances.

Reconciling EFT transactions, from the previous day, on a daily basis is a means to detect fraudulent transactions. An entity would verify its total EFT activity from the previous day with their financial institution’s records. If the totals don’t match, then one would match-up each transaction from the entity’s list to the bank’s until the exceptions are identified.

Aside from the controls mentioned above, other “best practice” preventative measures include the following:

- Change passwords frequently
- Use encryption software
- Use strong anti-virus protection software
- Stress caution to employees when opening e-mails and links



EFT fraud is a risk to many more businesses every day, especially smaller ones, as online and electronic banking becomes more prevalent in day-to-day operations. We recommend all businesses exercise common sense fraud prevention measures as part of any e-banking automation. A useful practice is to gain an understanding of their EFT process, and assess where the risk lies to determine the most effective controls to prevent, detect, and deter this type of fraud. Please contact Komisar Brady should you want our assistance in designing fraud prevention measures.

www.komisarbrady.com