

AUTOMATIC CLEARING HOUSE (ACH) AND WIRE TRANSFERS FRAUD INFORMATION FOR COMMERCIAL BANKING CLIENTS

Electronic Payment Fraud - How does it happen?

There are many ways information can be compromised and used to execute Electronic Payment Fraud (EPF) through ACH and Wire Transfer transactions. Knowing what to look for is an important first step to successfully defend against them.

Backdoor Methods

A hidden method for bypassing normal computer authentication systems

- ◆ *Keystroke Logging and Form Grabbing* - Zeus and SpyEye Trojans are very prevalent types of malicious software that steal information by capturing the information you type in.
- ◆ *Fraudulent websites, advertisements and email* - Spammers send emails claiming to be from government agencies or other legitimate sources such as the IRS and FBI. Criminals buy ad space and put up websites that try to collect your information or give you malicious software.
- ◆ Accessing internal network systems with inadequate controls.

Frontdoor Methods

- ◆ *Social Engineering* - Your employees may be called or emailed by an information thief posing as a First Midwest Bank employee to acquire secure information such as user IDs and passwords to be used in EPF.
- ◆ Phone and email solicitation
- ◆ *Internal Theft* - Credentials not properly protected can be stolen and used or sold by cleaning crews, visitors, vendors and even your employees.

Protecting Your Business - What precautions can you take?

Here are some basic steps you can take to supplement your business' information security:

- ◆ Perform inspections of your computers and network often . . .
 - Check to make sure your virus protection and detection
 - Require routine updates/patches to your network by your Information Technicians
- ◆ Never share passwords or authentication device information
- ◆ *Limit access* - Consider using a dedicated PC only for banking inquiries and access
- ◆ Use dual control for processing transactions and reconciliation - one person to initiate the transaction and a different person to approve it.
- ◆ Review account activity frequently (daily is recommended)
- ◆ Review payroll files for accuracy and changes, paying particular attention to payees and amounts.
- ◆ Limit administrative rights and employee access to systems and bank account information
- ◆ Consider obtaining insurance against unauthorized transactions (employee)

MORE PRECAUTIONS CONTINUED ON THE NEXT PAGE 

AUTOMATIC CLEARING HOUSE (ACH) AND WIRE TRANSFERS FRAUD INFORMATION FOR COMMERCIAL BANKING CLIENTS

Protecting Your Business - What precautions can you take? (Continued)

- ◆ Limit employees' ability to web surf or view personal emails and instruct them not click on unsolicited emails or links that appear suspicious
- ◆ Scrutinize web page URLs used to enter information
- ◆ Inform your bank at the first signs of suspicious activity

How does First Midwest protect your business' information?

At First Midwest, we closely monitor all transactions and verify those transactions with our clients via phone. We continually research current fraud and information theft methods, constantly updating our already multilayered fraud prevention program with additional controls to provide your company with the most up-to-date security measures such as Out Of Band Authentication solutions. Finally, our staff undergoes a high level of security training, making them a valuable resource in addition to our client information security awareness resources at firstmidwest.com/safe

Visit FirstMidwest.com/Safe for the most current resources on a wide array of information security topics for your business.