REGIONS
Treasury Management **Advisor**
Issue 107


# Preventing Payment Channel Fraud: Common Tactics and Defense

## Ensuring that internal controls and strategies are in place helps protect financial assets

The Federal Bureau of Investigation and U.S. Secret Service have recently issued new warnings in regard to the threat known as Business Email Compromise. Corporations and small business alike continue to face growing concerns as the fraudulent use of payment channels has increased. Understanding the changing tactics and channels fraudsters employ to perpetuate fraud is the first step toward prevention. Ensuring that internal controls and strategies are in place also will help protect financial assets.

For those who have not already considered the solutions available to help neutralize the threat, electronic payments could be at high risk. Wire payments continue to be an attractive vehicle for criminals due to the speed and finality of settlement, coupled with the fact that wire originators and volume continue to grow, making the collective target even larger.

### Tactics

Common schemes for payment channel fraud include fake vendor invoices sent via email and social engineering, as well as fraudsters demanding requests that require immediate action and confidentiality from the initiator. Compromised login information and forged email messages are two of the most common ways fraudsters commit financial crimes. As such, be cautious when acting upon any type of payment instructions received via email, even if the email appears to originate internally within your own company or from a known trading partner, as this could be an attempt at impostor fraud.

In the case of social engineering, a criminal persuades the victim to take a particular action, such as sharing private information or even wiring money. This is often done via email, a technique known as phishing. Matthew Speare, executive vice president at Regions Bank, explains that an increasing number of business owners are falling for this type of scam, in part because fraudsters have gotten more sophisticated and targeted in their approach. “They have done their research on your business,” he warns. “They are going to be convincing, so you have to be on guard. We have seen examples of incredibly well-done phishing emails, and we have seen customers lose millions. It can be devastating.”

In February 2015, a controller of an Omaha-based company lost $17.2 million due to an allegedly fraudulent email designed to look like it came from the CEO. That company is not alone. McAfee found that only four percent of

continued

## did you know?

Small businesses are facing unprecedented levels of fraud. According to the Association of Certified Fraud Examiners (ACFE), the typical business loses five percent of revenues each year to fraud. The latest ACFE study* found that nearly one in three small businesses experienced fraud in 2014, with a median loss of $154,000.

*Association of Certified Fraud Examiners, “Report to the Nations on Occupational Fraud and Abuse,” 2014, pg. 4, http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

REGIONS
Treasury Management **Advisor**
Issue 107

# reporting fraud

Immediately report anything you feel is suspicious, including emails that appear to be from your financial institution, application pop-ups, unexpected error messages or any unfamiliar login screens.

If you are a Regions client and suspect fraud or have received a suspicious communication, call Regions Client Services immediately at 1-800-787-3905.

# learn more

**Resources for defending against payment channel fraud:**

- Visit regions.com/stopfraud for fraud prevention resources, including best practices and bulletins from the FBI & U.S. Secret Service
- Visit regions.com/onlinesecurity for simple and effective online security hints and more information about dual control approval for ACH and wire transactions

executives worldwide could tell the difference between a real email and a phishing email 100 percent of the time.

## Impostor fraud growing in popularity

Impostor fraud involves a fraudster masquerading as a person whom you know and trust, such as a company executive, a vendor or, in some instances, even the IRS. The impostor makes contact via phone, email, fax, or mail and submits an invoice or requests a payment or a change to vendor payment instructions. If you follow the request based upon the perceived trusted relationship, any payments sent go to the fraudster instead of the intended party.

Imposter fraud differs greatly from a fraudster stealing online banking credentials and using them to make fraudulent payments. With impostor fraud, the organization's authorized users make the payments, so they appear as normal payments to the bank. This typically means the fraud is not quickly identified, which makes it harder to recover the funds, particularly if sent by wire. It is very important to us, as a trusted financial advisor, to help caution against such schemes.

## Avoid risky business, avoid business email compromise

- Avoid using open source email. The Internet Crime Complaint Center (IC3) cites open source email as the most common email type targeted by cybercriminals for business email compromise.
- Individuals responsible for handling wire transfers within a specific business are targeted by role, title or even name. Be alert.
- Spoofed emails appear as legitimate email requests. However, take a second look. Is the email address itself a "knockoff" with one letter missing, for example, to appear legitimate at first glance?
- Fraud is becoming more sophisticated daily. For example, fraudulent email requests for wire transfers are often error-free, well-written, and business-specific, and they do not raise suspicions to the legitimacy of the request.
- Victims of fraudulent email requests report request triggers, such as "code to admin expenses" or "urgent wire transfer/request."

continued


continued

REGIONS
Treasury Management **Advisor**
Issue 107

- The Internet Crime Complaint Center reports that most fraudulent wire transfer requests are business-specific, appearing as normal business transaction amounts to avoid raising red flags.
- Fraudulent emails commonly align in timing with the travel dates for business executives whose emails are spoofed so that fraudsters increase their chance of success.

## Mitigating the threat through easily implemented tactics

- Educate employees and have a multi-faceted fraud prevention plan. Fraud education and awareness is key. Make it a part of regular business communication to keep daily vulnerabilities top of mind.
- Have a fraud mitigation plan and prepare for the worst-case scenario.
- Promptly update business software.
- Always use a company website domain and company email accounts, not free, web-based email accounts.
- Take heed where business-related information is posted on social media and company websites, including job duties, descriptions, reporting structure, and out-of-office information.
- Monitor network traffic for anomalous activity.
- Always question urgent or pressured monetary requests.
- Use "Out of Band" communication tactics. For example, always use a secondary means of authentication to verify the legitimacy of financial transactions, such as confirming requests by telephone. The IC3 suggests arranging second-factor authentication early in business relationships so that the communication occurs outside the email environment to help avoid interception by a hacker.
- Do not give malware a chance. Always delete email from unknown originators. Do not open spam email, click on links within the email, or open attachments.
- Do not use the "Reply" option to respond to business emails. Make it a habit to use the "Forward" option instead, and either type the correct email address or select it from your address book.

## did you know?

> The window for recovering funds fraudulently procured through tactics like business email compromise can be hours, when recovery is even possible.

> A growing trend noted by the FBI is that cybercriminals are choosing to leverage publicly available information and vulnerabilities in corporate email systems to trick businesses into transferring large sums of money into fraudulent bank accounts, often internationally where recovery of funds is nearly as difficult as with cash payments. Over $1 billion was lost by companies worldwide from October 2013 through June 2015 as a result.

> More and more companies are choosing to put cyberinsurance policies in place. While a good idea for some, this is an emerging safeguard, and companies should first appropriately ascertain the true implications of a fraudulent occurrence as well as the measurable impacts.