BUSINESS EMAIL COMPROMISE

A CASE STUDY AND BEST PRACTICES

By Paul Happach, Senior Vice President, e-Channel Product Manager, Pacific Mercantile Bank

In their latest Payments Fraud and Control Survey, the Association for Financial Professionals found that 74% of the organizations surveyed reported they were victims of payment fraud in 2016. Are you taking steps to protect your business?

While check fraud remains the payment method of choice for fraudsters, wire fraud is the second most common method for the second year in a row, outpacing credit card and ACH fraud. Wire fraud can take many forms, but the predominant method being used is Business Email Compromise (BEC).

Let's consider an actual case study from Pacific Mercantile Bank. Could this happen to you?

CASE STUDY: EMAIL ACCOUNT TAKEOVER

Recently a relationship manager in one of our lending areas received an email from the CEO of one of their clients. The email text is below:

I am closing on a new property tomorrow and would be needing $90,115.00 to my ABC Bank account to complete the transaction. I'm in doubt that you have my ABC Bank on file, do I forward immediately?

The relationship manager recognized that this was an unusual request, but the email address appeared to be the correct email for the CEO of this client. The relationship manager received an additional email with the ABC Bank account information, followed by an email instructing the relationship manager to debit the client's line of credit.

The relationship manager recognized several red flags in these emails:

- This client uses online banking to send wire transfers, and had never requested a wire transfer via email.
- Email is not an acceptable channel for requesting wire transfer payment instructions.
- The client requested that funds be transferred from a line of credit that was only used for operating expenses. It was not used for property or real estate.

The relationship manager immediately reached out to the client via a phone call to discuss and confirm the request. The client replied that they had not sent any of the emails.

The issue was reported to our Information Technology department, which then assessed that the client's email account had been compromised. All incoming emails to the client were being redirected to a Gmail account not associated with the company. The fraudster was also able to send emails using the client's email server. Thus all fraudulent emails appeared to be legitimately originating from the client.

The client was notified of the compromise and Pacific Mercantile Bank worked with the company's Information Technology department to resolve the issue.

BUSINESS EMAIL COMPROMISE

This case study bears many of the earmarks of BEC, also known as CEO Fraud. These scams use email and social engineering to pose as a senior manager in order to trick employees into sending "urgent" and "confidential" wire transfers directly to the fraudsters' accounts. Here are some techniques the fraudsters may use.

EMAIL ACCOUNT TAKEOVER

The thief uses phishing or other means to install malware on an executive's computer and gains access to the executive's email account. Once they have this access, the thieves will take time to understand the organization's relationships and learn about the processes at the business for wire transfers, money movement, and vendor relationships. Then they use the compromised email account to create a money transfer request. The fraudsters continually monitor the email account and reroute emails questioning the wire transfer. The real executive is unaware of the request email and any email responses from employees.

LOOK-ALIKE DOMAIN

The fraudster may also use publicly available information to learn about the organization's executives and activities. They will typically send emails to executives in an effort to receive out-of-office replies and understand when an executive will be travelling. They create a domain that looks similar to the victim company domain. Then they use the look-alike email address, plus the information they have gathered on the business, to instruct fraudulent funds transfers.

FORGED VENDOR INVOICE

Fraudsters may also target an organization's vendor relationships. To forge a vendor invoice request, the fraudster may compromise an email address from the vendor, or from an individual within the company's finance department, to gain insight into typical invoice and payment patterns. With that information in hand, the fraudster will either use a compromised email account or look-alike domain email account to submit an invoice for payment to the fraudster's account rather than the vendor's.

CONFIDENTIAL AND URGENT

Thieves may also craft an elaborate story about the need for extreme urgency and high confidentiality. This story is designed to persuade the employee to act quickly and secretively, often with disregard for company safeguards and practices.

BEST PRACTICES

In addition to entrusting your business accounts to a bank that will take the time to get to know your business, understands the risk of payment fraud, and trains their relationship managers to be alert to the warning signs of fraud, businesses can take a number of positive actions to reduce the risk of falling victim to BEC.

DUAL CONTROL

Establish dual control for all money movement activities. Ensure that all funds transfers require a transaction creator and a separate approver. Utilize online banking security features to set additional approver levels for larger dollar transactions. Set up online alerts to notify approvers when a money transfer request is awaiting approval. Utilize the approval feature within your bank's mobile application to ensure that senior management can approve transactions on-the-go.

CONFIRM ALL REQUESTS

Instruct employees to always confirm requests for money movement, using a channel different from that used to make the request. For example, an email request should be followed up with a telephone call to the requestor.

CONTROL PUBLICLY AVAILABLE INFORMATION

Exercise restraint when publishing information regarding employee activities. Fraudsters may use this information to determine ideal time frames for committing fraud.

EDUCATE EMPLOYEES

Ensure employees are aware that this type of fraud is a real threat. Educate employees on the proper process for initiating money transfers, and enforce this process with all requests. Coach executives to encourage verification of all wire transfer requests. Encourage executives to introduce themselves to the Accounts Payable team and let them know it is acceptable to question any payment request.

INVESTIGATE BANK INQUIRIES

Often this type of fraud will trigger alarms at your bank. When the bank contacts the business to confirm the authenticity of a wire, the company employees may be tempted to confirm the wire as legitimate since it appears to have originated from an executive's request. Thus, the wire transfer is processed even though the bank questioned its authenticity. If the bank calls regarding a wire's validity, instruct employees to take this as a warning sign to be doubly sure that the wire is accurate and valid.

WHAT TO DO IF YOU ARE A VICTIM

The FBI and all financial institutions take this new threat very seriously. If you become a victim of this type of fraud take the following steps regardless of the dollar amount of the loss.

- Contact your financial institution immediately and request that they contact the financial institution where the funds were sent.
- File a complaint with the FBI's Internet Crime and Complaint Center (IC3). www.ic3.gov/complaint

SOLUTIONS TAILORED TO YOUR NEEDS

At Pacific Mercantile Bank, we have the expertise to evaluate your unique needs and determine the solutions that may help you avoid costly fraud losses. Call us today for a review of tools available to mitigate fraud risk.

PACIFIC MERCANTILE BANK

EQUAL HOUSING LENDER

FOR MORE INFORMATION CONTACT

Member FDIC

Cindy Verity - 858.320.8419
Cindy.Verity@pmbank.com

Shamara Vizcarra - 714.438.2629
Shamara.Vizcarra@pmbank.com