AMANDA DERCOLE
KEYBANK

Commercial Fraud Trends
Introduction

One of the best ways to combat fraud is for you and your employees to become experts in the ways fraudsters try to gain access to your information and exploit your natural instincts to be helpful. By familiarizing yourself with the scenarios to follow, you will be able to recognize and stop scam attempts in their tracks.
Recognizing Types of Fraud Scam Attempts
Business Email Compromise (BEC)

Business email compromise (BEC) is a type of email cyber crime scam in which an attacker targets businesses to defraud the company. Business email compromise is a large and growing problem that targets organizations of all sizes across every industry around the world. BEC scams have exposed organizations to billions of dollars in potential losses.
**Business Email Compromise Timeline**

An outline of how the business email compromise is executed by some organized crime groups

---

**Step 1: Identifying a Target**

Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

**Step 2: Grooming**

Spearphishing emails and/or phone calls target a victim company’s officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees’ human nature.

Grooming may occur over a few days or weeks.

---

**Step 3: Exchange of Information**

The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

*Note: Perpetrators may continue to groom the victims into transferring more funds.*

---

**Step 4: Wire Transfer**

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.
Business Email Compromise (BEC)

- Fraudster sends email that appears to come from the client and may look legitimate.
- The fraudster will request action on account or service (add new user to online wire service) or may ask to change payment instruction for wires or ACH transfer.
- May be committed in conjunction with claim settlement/vendor payment fraud.
Social Engineering

- Includes phishing (email), vishing (voice call), or smishing (SMS/Text)
- Fraudster misrepresents themselves as a legitimate business vendor, service provider, or other business partner in attempt to gain access to the client’s computer and/or obtain sensitive information
Account Takeover: Mobile & Online Banking Fraud

- Fraudster gains access to one or more online users’ sign-on credentials and has attempted or been successful with sending funds to a fraudulent account.
Malware

- Software unknowingly installed on the client’s computer specifically designed to harm and/or gain unauthorized access to data that can be used for financial gain

Ransomware

- Client’s access to computer operating system is blocked by means of malicious software until fee is paid to attackers
- Generally aimed at individuals, but becoming more prevalent with business entities
Claim Settlement/Vendor Payment Fraud

• Fraudster instructs insurance client or vendor to change the service provider’s settlement account

• Unauthorized account change permits the fraudster to direct large dollar ACH transactions to the fraudulent settlement account
Check Fraud

- Thieves steal checks from Post Office blue boxes, wash checks, and may change payee names and/or amounts.
Business Identity Theft

- Thieves steal checks from the mail payable to businesses and send them to a network partner.
- Partner registers a business within a different state, adding themselves as the owner or authorized party.
- Fraudster opens a business account and deposits the stolen check.
Protecting Yourself
Protecting Your Information

- Be mindful of the information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.

- Don’t click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing) and call the company to ask if the request is legitimate.

- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
Protecting Your Information

- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.
Stop Fraud Before it Happens

- Be wary and skeptical of unsolicited emails, phone calls, and text messages asking for information or requesting clicks on links.
- Hold all employees accountable for risk management and fraud protection.
- Initiate payments using dual controls.
- Never reveal passwords or responses to security questions to ANYONE including bank employees.
- Create a strict "password privacy" rules to ensure employees do not share credentials or passwords with other employees.
- Make sure your bank is promptly informed of changes in authorized officers, signers or online commercial users.
- Never access banking online platforms from an internet/web search.
- Be sure employees know the names of their relationship team, and have access of the relationship team’s phone numbers.
- Enroll in fraud protection products, such as Positive Pay or Electronic Payment Authorization (EPA)*.
Reporting Fraudulent Activity

- Regardless of the type of fraud, it’s vitally important to report as soon as it’s discovered.
- Contact your financial institution to report the fraudulent transactions so they can take action to help secure the account and/or assist with attempts to recover lost funds.
- File a police report to document.
THANK YOU