COMPEER FINANCIAL

PROTECT YOUR FINANCES:
UNDERSTANDING COMMON FRAUD ATTACK RISKS

Fraudsters are constantly devising new ways to exploit vulnerabilities and access sensitive information. Stay ahead of fraud by familiarizing yourself with some of the most prevalent attack risks related to money movement.

Invoice/Wire Fraud

Have you ever received a suspicious email or call from a vendor requesting a change in payment details? You might be a target of invoice or wire fraud. Fraudsters pose as vendors, aiming to trick individuals and businesses into redirecting payments to the fraudster's accounts—whether it's an electronic payment or a request to mail a check to a different physical address. With mailed checks, fraudsters can create counterfeit checks using your legitimate check as a template.

Hackers may breach a company's email system to study the accounts payable process and create a fraudulent invoice that appears legitimate, except for subtle changes to the payment instructions. A hacker can also breach a vendor's accounts receivable system and generate a fraudulent invoice or payment request. Similarly, a fraudster can take control of or spoof the email account of a company vendor.

ACH Debit Fraud

With just your account and routing numbers, fraudsters can initiate unauthorized electronic withdrawals. Using a vendor's online payment functionality, the fraudster enters the account number and bank routing number as their own and pays their bill. Be wary of unauthorized transactions that may appear on your statement.

Check Fraud

From check washing to counterfeiting, fraudsters have various tactics to exploit checks. Protect yourself by safeguarding your check stock and diligently monitoring your accounts.

Check Washing/Alteration

Fraudsters change the payee name, check amount, or both by removing or "washing" the original information and inserting new details. The altered check is then cashed under a falsified name while flowing through the banking system with original account and bank routing numbers.

Counterfeit Checks

Fake checks are created using genuine account and bank routing numbers for an individual or company. Using common printing technology, fraudsters generate checks, sometimes with the company's logo, and add a payee name and amount. While check stock security features help prevent alterations, they do not protect against counterfeits.

Payee Endorsement

Fraudsters intercept checks, forge the payee's endorsement and deposit or cash them. In some cases, checks may be electronically deposited without any endorsement. This theft may go unnoticed for weeks or months until the intended payee realizes the payment is missing.

Lost or Stolen Checks

Scammers may easily steal issued checks and new blank check stock from unsecured postal mailboxes, providing them with the materials to commit check fraud.

PROTECT YOUR FINANCES:
UNDERSTANDING COMMON FRAUD ATTACK RISKS

Impersonation Scams

Scammers conduct meticulous research to assume false identities and establish credibility, employing the right tone and language to convince their victims to take action.

Executive Impersonation
Many impersonation scams target high-ranking executives, such as CEOs or CFOs, by gaining control of or "spoofing" their email accounts. This involves creating fake email domains that closely resemble legitimate ones. Scammers then issue requests for ACH or wire transfers, often impersonating executives to lend credibility to their demands. Employees, believing the requests are genuine, unwittingly initiate transactions, putting company finances at risk.

Client Impersonation
Fraudsters may also target the email accounts of clients or vendors you work with to gather sensitive information for future scams. These requests may not necessarily involve payments but could be used to facilitate fraudulent activities down the line.

By understanding these common fraud attack risks, you can take proactive measures to protect your finances and sensitive information. Stay vigilant and always verify any unusual requests for payment or changes in payment instructions.