PREVENTING COMMON BUSINESS FRAUD

Keeping Your Business Safe

October 2022

Kevin King

CFE, CAFP, MBA

SVP, Director Enterprise Fraud Management
Atlantic Union Bank

ATLANTIC UNION BANK
CULTURE OF EXCELLENCE

We are
CARING.
COURAGEOUS.
COMMITTED.

Kevin brings over 20 years fraud, risk, technology, and regulatory compliance experience to his current role at Atlantic Union Bank as Director of Enterprise Fraud Management.

Areas of concentration:

- Fraud Detection and Prevention
- Fraud Risk Mitigation
- Fraud Investigations

Topics for Discussion

- Payment Redirection Fraud
- Business Email Compromise (BEC)
- Payroll Redirection Fraud
- Check Fraud
  - Counterfeit Checks
  - Altered Checks
  - Stolen/Forged Checks
- Account Takeover

Payment Redirection Fraud

Fraudsters impersonate your **vendor or supplier** and send you a payment change notice.

- The change notice instructs your staff (usually through email) to send payments to a different bank account that is controlled by the fraudsters.
- Staff believe they are following directions.

Multiple payments could be sent before the real vendor or supplier notifies your staff that payments are in arrears.

Atlantic Union Bank

Three Steps to Prevent Payment Redirection Fraud

1.Develop payment change notice procedures and implement a response process.

Train payments staff so they are aware of payment redirection fraud and how to react to possible threats.

2.Check the sender's email address carefully whenever a payment change notice is received via email.

3.Verify the change by contacting a known partner at the vendor or supplier, preferably by phone.

Employees should use a verified phone number or email address for the vendor NOT the contact information included on the payment change notice.

Business Email Compromise

SCENARIO:

You, the controller for a small business, get an early-morning email from the President of the company who is on vacation for a week. The correspondence is from her personal email address, instructing you to wire a certain amount of money to a particular destination.

Great news! The funds will solidify a deal the President has been engaged in for months. The email indicates the documents will be forthcoming. You dutifully process the wire as instructed by the President.

When the President phones on Friday to check in, you remind her to send the paperwork. She replies, “What paperwork?”

Atlantic Union Bank

Three Steps to Prevent BEC

- **Develop internal payment request procedures** and implement a response process whereby no Wire or ACH is sent based solely on an emailed request… by anyone.

  Based on the size of your organization, initiating payments via a verbal request may go a long way toward preventing this kind of fraud.

- **Check the sender’s email address carefully** whenever a payment request is received by email.

- **Verify the request by contacting the person** requesting the payment by a known phone number, NOT the phone number provided in the request.

  Fraudsters prey on the fact that staff may feel uncomfortable calling their company President’s personal phone number(s).

Watch Those Email Addresses!

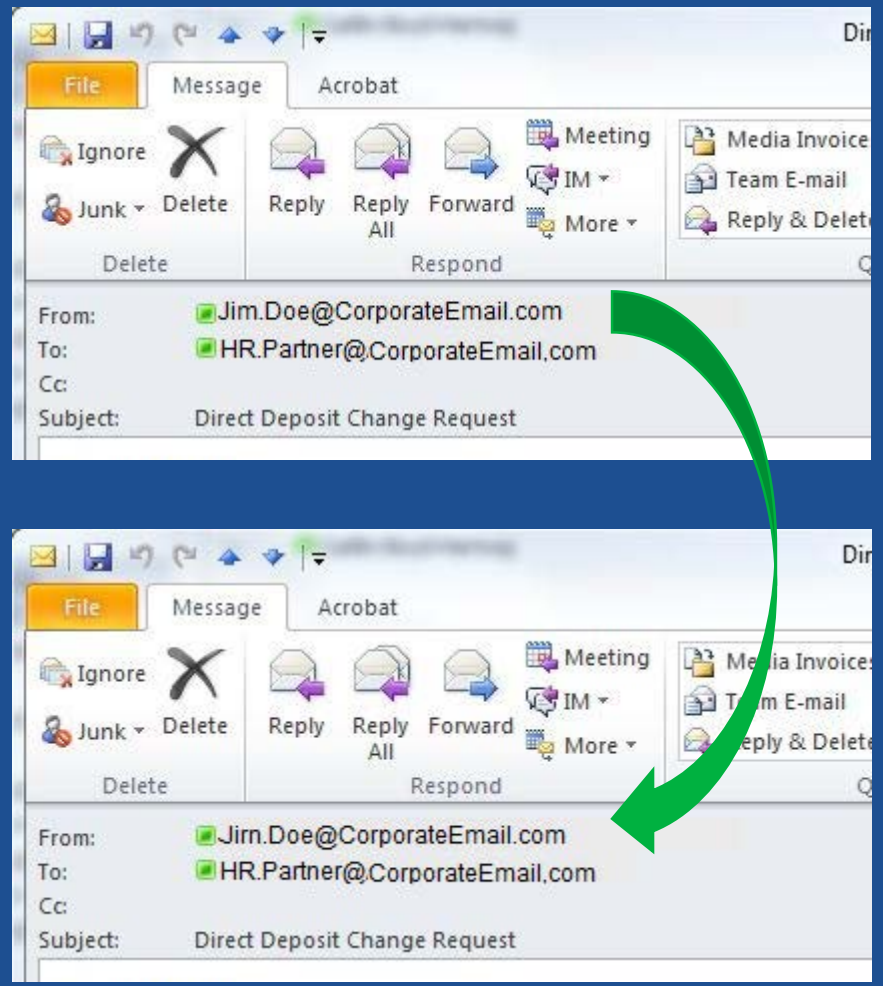
Watch for Spoofed Sender Email Address!

The fraudster **creates a new email address** that appears to be the same but has minor changes.

Most people don't catch the differences.

Be careful of email addresses with the letter "i" and "l", especially when they're together in sequence.

Equally tricky is when the letter "r" is followed by the letter "n", it looks just like an "m".



Atlantic Union Bank

Payroll Redirection Fraud

Fraudsters impersonate your **employee** and request changes to a direct deposit.

- The request (usually through email) instructs your payroll staff to send the direct deposit ACH to a different bank account that is controlled by the fraudsters.
- Staff believe they are following directions.

Multiple payrolls could be sent before the real employee notices that their checking account is overdrawn.

Three Steps to Prevent Payroll Redirection Fraud

1.Develop payroll direct deposit change request procedures and implement a response process.

Train payments staff to be aware of payroll redirection fraud and how to react to possible threats.

2.Check the sender's email address carefully when a payroll direct deposit change request is received via email.

Alternately, prohibit such changes from being made via email.

3.Verify the change by contacting the employee, preferably by phone.

Employees should use a verified phone number to contact the requestor, NOT contact information included on the payroll direct deposit change request email.

Types of Check Fraud

- ✓ **Counterfeit Check Fraud:** Using information from a business bank account, checks are printed that resemble the business's genuine checks.

✓**Altered Check Fraud:** Checks are altered by fraudsters after the check is legitimately filled out.

A fraudster may 'wash' the check (erase information) and enter new information on the check – typically the payee and/or the amount of the check.

✓**Forged Check Fraud:** Blank checks are typically stolen and the owner's signature is forged.

Preventing Check Fraud

- ✓ **Preventing Counterfeit Checks** is difficult because any individual with your account information can create checks that resemble your legitimate checks. Prevention is difficult, early detection is key. Minimize using multiple checkbooks.
- ✓ **Prevent Altered Checks** by maintaining control of checks sent out to suppliers/vendors from the time the checks are written to the time they're brought to the post office or picked up by a mail carrier.
- ✓ **Prevent Forged Checks** by maintaining control over check stock.
  - ✓ This is especially critical during times of crisis when controls over checks might be relaxed.
  - ✓ Fraudsters seldom take the check on top, as that would be too noticeable.

Detecting Check Fraud

Detecting most types of check fraud is easier with a product called **Positive Pay**.

- ✓ Positive Pay is an automated service that matches the information on presented checks (check number & dollar amount) against a list of checks provided by the business.
- ✓ Additional services called **Payee Positive Pay** will review payee information on presented checks to ensure the check is negotiated by the intended payee.

Absent Positive Pay, the best way to detect check fraud is by **continuous monitoring** of transactions against your account.

(The Bank offers ACH Positive Pay for electronic transactions)

The sooner you inform your banker of check fraud, the sooner your banker can act!

Corporate Account Takeover

Fraudster gains access to the corporate account(s), usually through breached privileges.

(Online Banking, Passcodes, Personal Information)

There are two common means for gaining access to an account:

1. **Credential Stuffing:** Perhaps the CFO's password was the same password she used for her Hotel Rewards account, which got breached.

   ➢ With credential stuffing, the fraudster uses that same password on the CFO's other accounts, including her corporate sign-in.

2. **Spear Phishing:** Fraudsters send targeted emails to privileged user of the corporate network, hoping they fall for the fraud and provide their account credentials.

   ➢ The fraudster uses this information to take over the account.

Prevention

1. **Use different passwords** for all of your accounts.
   At the very least, do not use the same passwords for your personal and business accounts.

2. **Don't click email links from unknown senders.**
   - Hover over the sender to see the full email address.
   - Be careful about emails that "bait the hook" with current events, such as a package delivery email around the holidays, flower delivery email around Valentine's Day, or emails about COVID.
   - FBI reports over $2.4B in fraud associated with Phishing and Business Email Compromise in 2021.
   - FBI reports ransomware continues to evolve from "big game" targets toward midsized organizations as awareness increases.

3. **Training:** <u>You can't over train staff</u> on how fraudsters try to access accounts. In addition to training, consider a phishing email test.
   - Many IT vendors offer phishing email testing campaigns.
   - Phishing email tests are very helpful in identifying who in your business needs additional training.

Contact Us

Contact us immediately if you suspect you've accidently redirected payments or payroll direct deposits to a fraudulent destination.

Customer Care: 800-990-4828
Mon-Fri: 7am - 8pm
Sat: 7am - 5pm

Thank You!

Appendix Q&A (1)

- If I am a victim of fraud, do I have to file a police report?
  - In some instances, like card fraud an affidavit or a police report won't be required for a fraud claim. Regulations regarding card transactions allow the bank to pursue recovery without written documentation. In some instances we may ask for proof that you engaged with a vendor or merchant in an attempt to resolve the situation, that documentation assists investigators with decisions on how to best attempt recovery on your behalf or the banks.
  - Other fraud types like wire fraud, check fraud or ACH fraud, most common to commercial clients, often require a police report and a bank approved notarized declaration of loss (affidavit). This documentation serves several purposes for the bank. Most notably for clients it expedites our ability to recover your funds from other financial institutions and confirms for all parties involved that our client is in fact a victim of some type of financial loss.

- Other than Positive Pay, how else can I protect my account and what are my risks?
  - Much like your personal account, daily monitoring of items posting to your account is critical, you effectively become your own form of positive pay. If a fraudulent item is found, call the bank immediately. We will begin the process to prevent additional fraud, document the incident, and begin the recovery process. The banks best opportunity for recovery is within the first 24 hours of the event occurring, it is imperative that you act quickly.
  - If your organization does not have the resources to perform daily monitoring, Positive Pay services provide the peace of mind knowing the bank can protect your financial assets.
  - If you decline to participate in Positive Pay, the bank would no longer be able to honor most fraudulent check claims against your account. We will aggressively attempt to recover lost funds on your behalf, but with no guarantees. In many instances those recovery efforts are an extremely time consuming process.

Appendix: Q&A (2)

- When I experience fraud, how quickly can I expect credit for my loss?
  - Ultimately, the faster you get us the documentation needed to investigate the loss, the faster we can resolve your case. Our goal is to complete your case within 30 days, but a timely return of your documentation will help move the case along and may result in a reduced resolution timeframe.
  - If we are acting on your behalf to recover a loss from another financial institution, we will credit your account once funds are received. Exchange of funds between financial institutions in some fraud cases are dependent on the completion of a fraud investigation at both institutions. Regulations allow up to 90 business days for completion of that process. Our goal is to credit your account within 1 business day of receipt of the funds.

- If I fall victim to wire fraud scam, what do I need to do to increase my opportunities for recovery?
  - Call the bank immediately. Fraudulent wire transactions often result in little to no opportunity for recovery. We will attempt a wire recall, but depending on timing this may not be successful.
  - In all instances of wire fraud after calling the bank you should quickly obtain a police report and report your loss to IC3.gov. Upon completion, update the bank with case numbers so investigators can document our investigation.
  - If the wire was transmitted internationally, you will be instructed to initiate the Wire Fraud Kill chain utilizing IC3.gov. The bank can not do this on your behalf, we can only assist Federal Law Enforcement once they are engaged.
  - Remember knowing who your wire is going to and having good procedures to validate the recipient is imperative to protecting yourself against wire fraud.

Appendix: Q&A (3)

- Why should I not use multiple checkbooks for my organization?
  - The use of multiple check books on the same account within your company often generates false notifications by tools used at the bank to protect you. False notifications may result in a delay in our response to potential fraud.
  - Positive Pay also becomes effective at preventing fraud when you use multiple checkbooks due to the possibility of duplicate check numbers or unexpected changes in the check number from one processing day to the next.
  - In instances where we are concerned about fraud on your account we may take action that impacts your transaction. Our goal is to minimize negative impact to your normal course of business. If we attempt to contact you regarding suspected transactions, a quick response on your behalf will help reduce that risk.

- How are criminals getting my information?
  - We have most recently seen stolen checks (car smash and grabs, theft from offices, etc.) as a leading trend within our footprint. Secure your checks and cards!
  - Stolen mail is an industry problem. Never leave outgoing or incoming payments in an unattended mailbox. It is a best practice to maintain control of your payments until your mail service provider takes possession of them. Theft of issued checks often results in alterations to the item for resale to a fraudster, negation of the item for cash in branches using fake identity, or visibility into your check stock for creation of future counterfeit checks.
  - Stole business critical information is most often result of vulnerable digital hardware, response to malware of phishing attacks, or intrusion into third party databases containing your information and utilized in the normal course of business.
  - Remember your clients are also often at risk for theft of business information also. Business email compromises (BEC) are the largest contributing factor for payment redirections for our commercial clients.