Fraud Prevention and Solutions to Mitigate Risk

Sandy Spring Bank

Rob Turano

Corporate Security Director, SVP

- Maryland State Police, Retired
- 27 Years in Law Enforcement
- Joined Sandy Spring Bank in 2013

Fraud Prevention

Sandy Spring Bank takes the protection of your personal information seriously, utilizing technology and other tools while also working with internal and external partners to diligently monitor and mitigate potential risks.

While we maintain comprehensive security procedures, it is also important for our clients to be well informed so that they may help us stop fraud before it even happens.

Corporate Security Responsibilities

Centralized security team specialized in fraud monitoring, investigations, and client outreach

- Analyzing daily fraud reports
  - Rules-Based and Behavioral (ML & AI) analytics
- Reviewing transactions
- Contacting clients – client engagements
- Ensuring physical and personal safety

Federal Trade Commission (FTC)

- The FTC reports 2023 record fraud losses exceeding $10 billion
  - The medical field, physicians, hospitals, like banks are highly regulated --- they are required to take steps to secure and protect client data, financial records, etc.
  - Consumers and industries being impacted and targeted through Business Email Compromises (BECs) and counterfeit checks
  - BEC --- also known as Email Account Compromise (EAC) --- is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business --- both personal and professional.

Business Email Compromise (BEC)

- One of the most financially damaging online crimes
- Criminals send emails with a request that appears legitimate
  - Vendor sending an invoice from an updated email
  - CEO asking to purchase gift cards for employee rewards
  - Title company sending wire instructions to homeowner

Versions of these scenarios happened to real victims receiving fake messages, resulting in thousands – or hundreds of thousands – of dollars being sent to criminals.

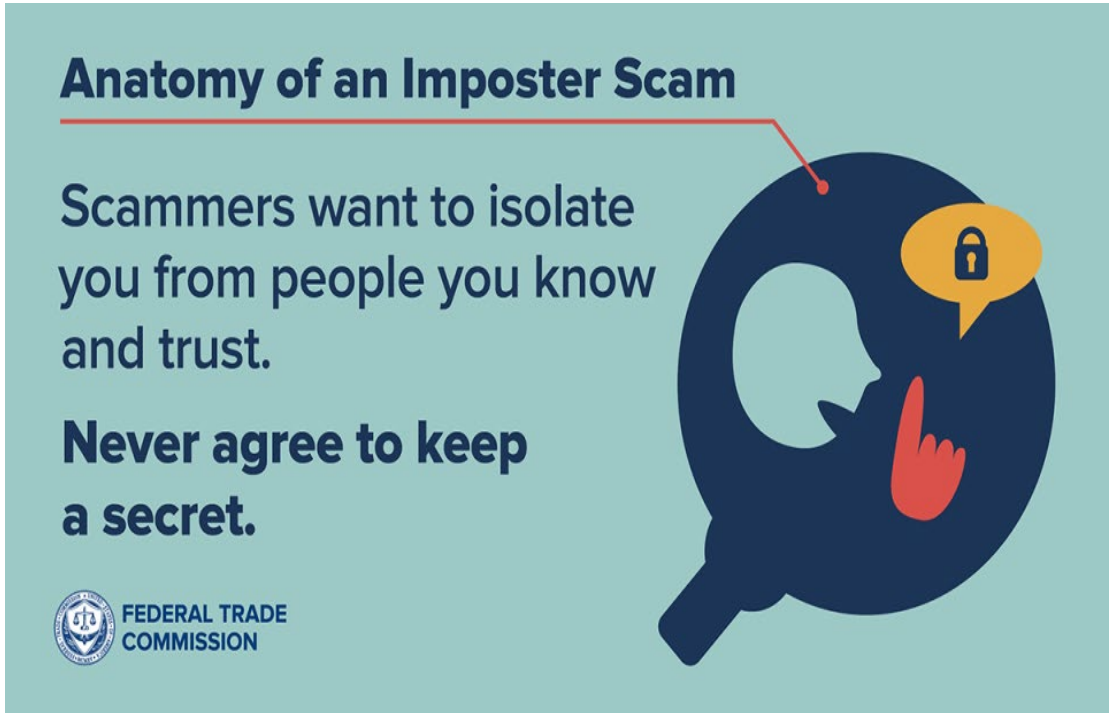
- BEC is the major cause of ACH & wire fraud

BEC Case Studies

- Business receives an email to change payment process and account information
  - How is it being verified?
- Business receives email to send a wire or ACH payment from CEO, CFO, when they are out of the office, vacation, business travel, etc.
  - How is it being verified?
- How is your email domain secured?
- Do you have an IT security vendor/partner?
- What are your internal office controls?
- Do you have a process?

BEC Case Studies

- Anatomy of an Imposter Scam



Counterfeit Checks

- High Volume = High Vulnerability
  - Stolen
  - Counterfeited
  - Altered

Options to eliminate and reduce counterfeit check fraud

- Reduce volume of checks issued
  - Online bill pay
  - Limit access
  - Secure mail
  - Vendor's access/exposure

- Bank's Payee Positive Pay
- Accept checks (Treasury & Government) through direct deposit

Credit Card Fraud

- Frank Abagnale – “Catch Me If You Can”
  - Criminal felon, FBI consultant
- Credit Card Protections
  - Regulation “E” – Regulation E implements the Electronic Fund Transfer Act (EFTA), which establishes a basic framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems.
  - Businesses are required to use chip enabled card readers
  - Who processes your Credit Card Transactions?
  - Consumer Protections – Card/bank issuers assume liability when used in compliance

Prevention and Reduction

- Establish protocols to mitigate risk
  - Dual controls
- Educate clients & employees on BECs
  - Verify requests or transactions through other channels
- Limit check access/control
- Secure check posting & distribution
- Use ACH payments
- Use Tokens
- Use MFA
- Consider bank services

Identity Theft & other Breaches

- Data Breaches
  - Equifax, Home Depot, OPM, Target
- Symptoms of a compromise:
  - Unexplained new accounts
  - Rejected for new credit
  - Tax return issues
  - Unexplained bills
  - Unexplained emails
- Email compromise
  - Check your trash bin

Securing and Monitoring Your Identity

- Request an annual credit report
- Place fraud alerts with your creditors/banks, etc.
- Use current fraud alert platforms
- Update and enhance security passwords
- Set up alerts on accounts and cards
- Review banking activity regularly/monthly
- Report all unauthorized transactions immediately/timely

Link: https://www.identitytheft.gov/

Presented by
Monica L. Tressler
Senior Vice President & Lead for Treasury Management & Commercial Banking
mtressler@sandyspringbank.com
571-421-7808

Protect Your Assets

With millions of checks and electronic payments in circulation each day, businesses don’t have the time or resources to inspect each individual transaction. Yet, no one can afford to ignore the fact that some of these transactions are fraudulent. Unfortunately, fraud isn’t usually detected until after the check or electronic ACH debit has been paid.

Preventing fraud with Check Payee and ACH Positive Pay services represent a proactive and effective approach to combating check and ACH fraud. As an early warning fraud detection system, Positive Pay services arm your business with the information needed to stop check and ACH fraud before it becomes a loss.

How does Check Payee Positive Pay work?

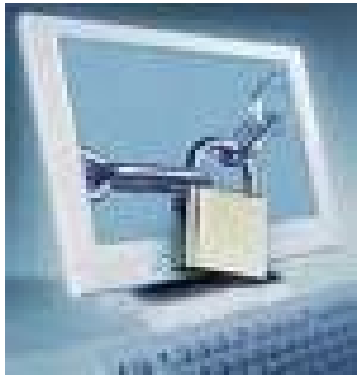
From high-tech counterfeit checks to simple forgeries, business checking accounts are targets for fraudsters. Check Payee Positive Pay allows you to electronically share (upload) your check issue file for all written checks with the Bank. We will only pay the checks listed on your check issue file according to precise specifications you provide, such as payee, amount, serial number, check date, etc. If a check is presented that is not on the issue file, the client will be notified and requested to make a “Pay or No Pay” decision within a set decision time window. If no decision is made, the default is to “return”, therefore mitigating fraud.

How does ACH Positive Pay work?

As check fraud has increased, so has electronic ACH fraud. ACH Positive Pay allows you to prevent unauthorized electronic debits from posting to your account by controlling who you will accept ACH transactions from. You can create filters to allow specific transaction types to post to your account and prevent other transaction types from posting to your account. You even have the ability to block specific transactions over a certain dollar amount. When alerted of an ACH transaction that was not preauthorized, the client will be notified and requested to make a “Pay or No Pay” decision within a set decision time window. If no decision is made, the default is to “return”, therefore mitigating fraud.

Internal Controls

- **Internal Controls**
  - Dual Administration
  - User Credentials & Limits
  - Appropriate Online Entitlements (Admin and User Level)
  - Out Of Band Authentication (OOBA) / Tokens / Soft Tokens
  - Dual Control – Segregation of Duties (Origination and Approval)
    - Profile level
    - Payments out the door
  - Phone Verification of Vendor payment details / Invoices
  - Securely kept bank account documents and check stock



Secure Soft Token

- **What is a secure token?**

  A secure token is a device that allows a user to prove their identity when logging into online systems or approving online transactions. Tokens are unique to each individual and may not be shared. Sandy Spring Bank uses RSA Authenticator (SecureID) Software Tokens for approving ACH and Wire Transfers through business online banking. The eight-digit code generated by the token, which changes every thirty seconds, is used in conjunction with a PIN to create a Passcode to approve these transactions.

  The RSA Authenticator (SecureID) Software Token is an effective tool to help prevent potential fraud attempts. The RSA Authenticator (SecureID) Software Token app is tied to an Invidia's physical device and not their phone number which should reduce the risk of account takeover.


Questions?