Presented by Onalee Arnold, Fraud Prevention Manager

PARK NATIONAL BANK

Industry Fraud Trends

Electronic fraud

- Types of electronic fraud customers experience include:
  - Debit card
  - ACH
  - Wire

Check fraud

- Types of check fraud customers experience include:
  - Counterfeit
  - Forged maker’s signature
  - Altered check
  - Missing endorsement
  - Forged endorsement
  - Remotely-created check

Current scams/fraud

Business email – compromise or redirect

Check fraud – stolen mail

Trust your suspicions

- Review previous communication received from the individual
  - Is the communication the same or different?
- Verify the request
  - In-person verification
  - Call the business or individual, using a phone number you have on file
- Review the request with a supervisor
  - Don’t make changes without confirmation
- Contact your bank for assistance
- Know the red flags

Red flags

- Spelling errors, poor grammar, and poor punctuation in emails or communication
- Urgency to complete transaction (can’t be reached by phone or traveling)
- Change or redirection of payment from original payment location
- Email address changes from previous communications

Known Industry Fraud Trends

SCENARIO #1

Redirect scam

A business sends a message from an email account that's slightly different from the company email address that's normally used. The message contains erroneous payment instructions. Additional verification is not obtained, and funds are transferred to a fraudulent account.

SCENARIO #2

Redirect scam

An employee sends a text requesting their payroll be updated to a new account and routing number. The employee creates a sense of urgency by stating they're traveling and stuck in another country.

SCENARIO #3

Account takeover

Business becomes a victim of online account takeover by giving online banking access to someone claiming to be with a reputable company such as QuickBooks, Dell or Microsoft. Scammer accesses online banking and collects account information to sends funds via wire or ACH.

SCENARIO #4

Check fraud

A fraudster steals checks from the mail. Legitimate checks are used to create counterfeit checks, oftentimes with washed payees.

SCENARIO #5

Business email compromise: Wire scam

Your company's accounts payable clerk receives an urgent email from a vendor instructing you to pay a past-due invoice via wire to a new account. The email is sent by the CEO who is traveling and can't be contacted. Since it's overdue, if it's not paid immediately, you'll be charged late fees.

Post fraud best practices

Investigation includes:

- Review accounts for past or additional suspicious activity
- Alerting the bank of the fraud incident
  - Affidavits may be requested as part of the recovery process
- Contacting law enforcement
  - Law enforcement may request footage from the bank
- Working with your IT team to scan and update your virus protection
- Responsibility for fraud loss depends on the outcome, account disclosures and agreements, products and services and legal outcomes.

Best practices for fraud protection

- Talk to your banker about tools like Positive Pay and ACH Debit Block
- Use additional online banking security available through your bank
  - Tokens (physical and soft)
  - Multi-factor authentication
  - Secure browser, stand alone computer
- Use banking alerts
  - Keep contact info current
- Replace checks with ACH and wire payments
  - Prevent account information from falling into the wrong hands
- Reconcile accounts often and report any suspicious activity to your bank/banker

PARK NATIONAL BANK

What questions do you have?