# ANB'S FRAUD AWARENESS & PREVENTION CHECKLIST

## Fraud prevention and risk management controls help protect your organization.

Fraud is an unfortunate reality for businesses. Not only can it be costly, but with each new advancement in technology, it seems a new fraud technique is invented. From check fraud to ACH fraud to the threat of cyberattack and data loss, no organization is immune from internal or external fraud. Use this list to aid you in taking thoughtful, preventative measures to reduce your exposure to fraud.

### Account Structure

- Minimize the number of accounts
- Use unique serial number ranges for specific purposes
- Segregate accounts at greater risk

### Anti-Malware

- Exercise extreme caution with any requests for account information or banking access credentials
- Immediately report any questionable account transactions
- Never leave a computer unattended while using online banking or investing service
- Never access bank, brokerage or other financial services information in public locations such as a library or coffee shop

### Antivirus and Spyware

- Do not open attachments or follow links in emails that were unsolicited or unexpected
- Do not download files from unfamiliar file-sharing sites
- Update your antivirus applications regularly and schedule antivirus software to run daily and automatically
- Install a firewall as a first line of defense against hackers with a default-deny configuration
- Utilize security certification verification software
- Utilize an intrusion detection system to monitor network and system traffic for suspicious activity
- Prepare, implement, and practice an incident response plan
- Install perimeter spam and malicious content filtering

# ANB'S FRAUD AWARENESS & PREVENTION CHECKLIST

## Banking Services

- Validate the legitimacy of checks presented by using Positive Pay
- Designate accounts for use in electronic transactions only and block checks from debiting
- Stop all ACH originators from debiting certain accounts by using ACH debit blocks
- Ensure only authorized ACH originators can access your accounts for predetermined amounts by using ACH debit filters

## Check Supply

- Use an established vendor
- Incorporate security features into check stock such as fluorescent fibers, watermarks, chemical resistance, bleach reactive stains, thermochromic ink and microprinting warnings
- Use a unique check style for each account type
- Use secured storage with controlled access for check stock, check printing equipment, endorsement stamps, and canceled checks

## Internal Controls

- Use dual authorization for all monetary transactions, including online ACH originations, ACH direct transmissions, wire transfers, and RDC
- Formally and regularly review internet and email security
- Set policies for passwords that include:
  - Unique passwords for each application
  - Passwords should not be easy to guess (e.g., pet or children's names)
  - Passwords should contain a combination of upper and lowercase letters and special characters
  - Passwords should be changed at least every 45 days
- Mask account numbers and EINs on correspondence
- Conduct surprise audits
- Never sign checks in advance
- Review and update signature cards annually
- Use dedicated, stand-alone computers for online banking
- Set policies to disable user IDs and passwords during extended vacations or leaves of absence
- Discourage pre-filling (or remembering) passwords and usernames at log-in

# ANB'S FRAUD AWARENESS & PREVENTION CHECKLIST

## Staffing

- Limit authorizations to appropriate employees
- Segregate duties between staff that issue payments and those that reconcile
- Rotate banking duties to prevent collusion
- Review system access privileges for all employees regularly
- Proactively provide education on phishing and other cybercrimes
- Screen and log temporary help and vendors that come on site
- Promptly deactivate employees' access cards for temporary or laid-off staff

## Transaction Controls

- Review and reconcile accounts daily and monthly
- Validate vendor legitimacy and account information by calling the vendor directly if an invoice is suspect or you receive a change of address request
- Formalize procedures to securely retain and then safely shred checks
- When possible, convert paper payments to electronic formats
- Implement policies requiring employees to log off computers when not in use
- Do not provide your EIN unless required for validated need
- Secure your check stock and other negotiable documents and manage under dual control
- Maintain ACH and wire transfer limits as low as possible

**For questions or more information on antifraud products, contact American National Bank's Treasury Services Team at 402-399-5037.**