AMERICAN NATIONAL BANK

Fraud Awareness and Prevention Checklist

PROTECT YOUR ORGANIZATION BY VERIFYING THAT YOU HAVE FRAUD PREVENTION AND RISK MANAGEMENT CONTROLS IN PLACE

Fraud is an unfortunate and permanent reality in business today, with the incidence and severity of fraudulent occurrences on the rise. Check fraud is still rampant and ACH fraud is increasing, with more corporations moving to electronic payments. And cyber fraud has just begun, with cyber syndicates as serious about their business as you are about yours. No organization is immune from either internal or external fraud. It is imperative that you take preventative measures utilizing both technology and common sense in the following areas:

Account Structure	Check Supply	Transaction Controls	Anti-Malware
Banking Services	Internal Controls	Staffing	Antivirus & Spyware Software

Account Structure

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

Check Supply

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

AMERICAN NATIONAL BANK

Transaction Controls

- Review and reconcile accounts daily and monthly
- Validate vendor legitimacy and account information by performing a call back if invoice is suspect or there is a change of address request
- Formalize procedures to securely retain then safely shred checks
- When possible convert paper payments to electronic formats
- Implement policies requiring employees to always log off and not wait for automated time-out
- 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

Anti-Malware

- Exercise extreme caution when confronted with any request to divulge account information or banking access credentials
- Immediately report any transactions in your account that you question
- Never leave a computer unattended while using any online banking or investing service
- Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc.

Antivirus and Spyware

- Do not open attachments to an email if the subject line or email itself looks suspicious or unexpected
- ie: IRS, BBB, UPS, etc.
- Do not download from unfamiliar file-sharing sites
- Aggressively update your antivirus applications regularly
- Install a firewall as a first line of defense against hackers with default-deny configuration

- Schedule antivirus software to run daily and automatically
- Utilize security certification verification software
- Employ intrusion analytics software
- Prepare, implement and practice an incident response plan
- Install perimeter spam and malicious-content filtering

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 security
- Set policies regarding passwords such that
    - Same passwords are not used for different applications
    - They are not easy to guess; e.g., pet or children's names, etc.
    - They contain special characters and not just alphanumeric
    - They are changed often
- Mask account numbers and EINs on correspondence
- Conduct surprise audits
- Never sign checks in advance
- Review and update signature cards annually
- Use only dedicated, stand-alone computers for online banking where email and web browsing are not allowed
- Set policies to disable user IDs and passwords during leaves and to discourage pre-filling passwords and user names at log-in

AMERICAN NATIONAL BANK

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

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 originator 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

Contact American National Bank's Treasury Services Team for antifraud products: 402-399-5037.