BB&T

Fighting Payment Fraud

A GROWING RISK

When it comes to payment fraud, perpetrators today are more wily than ever, forcing businesses to increase their methods to protect themselves from significant financial risk. Today, an estimated 80 percent of companies have experienced payment fraud or fraud attempts. The cost to U.S. businesses and their customers totals billions of dollars annually, and the number of incidents continues to grow at an alarming rate.

Types of Fraud

Fraud can come from anywhere, including inside. Here are some examples of how fraud can occur:

- **Executive impostor.**
  This is when a fraudster poses as an executive of your company. For example, a chief financial officer received an email purportedly from her CEO requesting $61,000 be wired to a bank account for a certain transaction. She sent the wire without noticing a slight difference in the domain name of the email.

- **Vendor impostor.**
  A fraudster poses as a vendor and requests changes in payment instructions. For example, a company was negotiating the purchase of cotton from a known vendor as a fraudster monitored their email. The fraudster tampered with the date on which the seller would expect to receive payment and the payment instructions. As a result, the buyer sent $41,000 to the fraudster's account.

- **Hacking accounts payable departments.**
  Criminals can breach the email of your company's accounts. They learn the patterns of requests received and use them to generate fraudulent invoices.

- **Embezzlement.**
  Whether it is malicious intent or simple negligence, fraud caused by employees can be an even greater threat than damage coming from the outside. One controller stole $600,000 by using online banking to connect her personal account to the business account. She started by charging purchases to the business card, moved to ACH payments and then to issuing checks.

A combination of better oversight, tighter payment controls and a dual-approval system may have helped prevent the examples above. But a truly effective cash-management platform needs a wide array of robust security features to protect assets, clients, trading partners and employees. A comprehensive data security plan includes training your employees and regularly reviewing with them the latest fraud trends to keep security on everyone's radar.

A truly effective cash management platform needs a wide array of robust security features to protect assets, clients, trading partners and employees.

Best Practices for Computer Systems and Online Transactions

Here are some ways to protect your computer and online systems from hackers and those looking to steal information:

Safeguard Your Systems

Install a dedicated, actively managed firewall, especially with a broadband or dedicated internet connection, such as DSL or cable. Regularly update this and other antivirus, spyware-detection software — as well as security patches — on all computer systems. Use industry standard products instead of those available for free.

Verify your browsers are connecting to all banking websites through a secure session, versus an unencrypted session, using HTTPS or Transport Layer Security protocols (websites with https://). This allows secured information to pass between the client (browser) and the server (website).

For greatest security, conduct online banking activities from a stand-alone, hardened and locked-down computer system.

Protect Data

Don't use online portal passwords or sign-on information with other websites or third-party vendors. Likewise, don't use automatic login features that save usernames and passwords with online banking applications.

Limit administrative computer rights, and access only trusted business websites during online banking to avoid accidentally downloading malware or viruses. Likewise, never access bank, brokerage or other financial services information from public or shared computers at internet cafes or libraries. Don't use public Wi-Fi networks, because fraudsters often target users to access online financial services. Never leave a computer unattended during online banking or investing sessions. Avoid all social media channels from company computers.

Establish procedures to identify and isolate network computers infected with malware. Make certain infected computers are fully remediated before using them again for online transactions.

> Make sure your financial institution has up-to-date email addresses and phone numbers.

Use Dual Approval and Real-Time Alerts

Require two or more users to create, review and release payments, set account limits and use multifactor, out-of-band authentication for changes.

Beware of prompts to enter your credentials that appear out of the usual sequence or application screens that show unfamiliar data fields along with a change in the look and feel of the page.

Set up a system to receive real-time alerts of unexpected or suspicious activity and transaction status changes. These include new-user setup, modification or deletion of accounts; password changes; pending payment and payment templates; transaction limit change approvals; Positive Pay exceptions; investment orders; account restrictions; administration modifications; and outgoing ACH/wire payments.

If you think you've been hacked, immediately report all suspicious transactions to your financial institution. Your financial institution might be calling you as well to validate transactions. Make sure your financial institution has up-to-date email addresses and phone numbers. Every minute counts with attempts to reverse and recapture lost funds.

Electronic Payment Best Practices

When it comes to electronic payments, there are a few easy steps you can take to make sure your money is going to the right place and not being intercepted by fraudsters.

- Set individual payment limits appropriate for the user, and use a maximum dollar amount per transaction for initiating and approving wires and transfers. In addition, set maximum daily cumulative dollar amounts for all wires initiated and/or approved.
- Review ACH and wire-transfer procedures regularly to ensure user entitlements represent appropriate needs. Use repetitive wire templates to eliminate manual intervention and manipulation. Add ACH blocks to stop incoming ACH transactions from posting to your accounts and require dual approval for all payment transactions.
- Use ACH Positive Pay, a cash management service that allows a user to view ACH exceptions and make decisions to pay or return their items.
- Create an ask-and-respond protocol using a PIN/password with payment or administrative changes outside standard operating procedures.
- Consider receiving ACH payments through a masked virtual UPIC bank account number and paying employees by reloadable debit cards.
- Implement the segregation of accounts, reconcile accounts daily and sign up for payment alerts.

Email Best Practices

Business Email Compromise, or BEC, is a popular vehicle for fraud. It's important to authenticate all suspicious email requests from superiors, agencies, vendors and colleagues through another communications channel. Curb faxing or emailing wire instructions to anyone.

Restrict access to personal email accounts, and match requests with known invoices. Ask: "Do I know the sender? Am I expecting a message from this company? Did I initiate action that would result in a response from the organization? What kind of change is the email suggesting?"

EMAIL DANGER SIGNS

Look for these signs that an email is fraudulent:

- Odd file attachments or links
- Grammatical errors, awkward writing, and poor visual design and different sequence of screens
- Emails that request account information or banking-access credentials, such as user-names, passwords, PIN codes or Social Security numbers
- Urgent appeals, such as threats of closing your account if you fail to confirm, verify or authenticate your personal information
- Messages about system and security updates and impending software upgrades may also be designed to trick users into providing sensitive company information
- Requests to change account numbers, update payments instructions or processing of an unusual amount at a strange time.

Check Payment Best Practices

Check fraud is both the oldest and most widespread form of financial fraud, according to the 2016 AFP Survey and Report. Checks may be stolen, copied or altered. Here are some protective actions:

- Reconcile accounts daily
- Segregate internal audit from controller duties
- Consider switching to electronic payments only
- Verify with other institutions the legitimacy of checks
- Safeguard check stock and use security features
- Consider outsourcing check processing to a secured vendor
- Use Payee Positive Pay or Positive Pay to compare presented checks against issued checks, with immediate alerts for exceptions

Constant Education and Assessment

Cybercriminals prey on companies when staff are not educated and proper procedures and controls are not in place. Scammers thrive on unpreparedness, as speed is important when successfully stealing business assets. Companies may have extensive security measures in place to prevent fraud, but they can still fall victim to cybercrime if their employees don't know how to stay vigilant. Conduct regular risk assessments on all your account and transaction needs.

It's critical to educate everyone in your organization to the signs of fraud. They must understand the purpose of security protocols, how to identify suspicious situations and what to do when anomalies arise.

If you believe your staff can't be fooled by ruses, test them to find out. Send an employee a nonstandard request pretending to initiate a change. How does your employee respond? Does he or she follow protocol? What is the outcome? How do you reinforce the correct responses?

It's important not only to test procedures, but also to share recent fraud events with employees as part of an effective fraud education program. Communicating these incidents is integral to successful fraud prevention.