Payments fraud prevention best practices

Take these steps to help build your payments fraud prevention program on a foundation of best practices.

The Uniform Commercial Code (UCC) requires businesses to observe “reasonable commercial standards” to prevent fraud. Establishing consistent fraud prevention practices is the first step in creating a fraud prevention program.

We offer the following best practices to help you create a payments fraud prevention program for your organization.

Define your fraud prevention program

Assess your payment fraud risk, segregate payments by account and apply appropriate bank solutions.

- Consider an integrated treasury management system with built-in fraud prevention.
- Convert from paper checks to electronic payments where possible.
- Regularly review fraud prevention best practices and solutions for effectiveness.

Manage employees and organize tasks

Educate employees to recognize fraud and separate account management and cash management tasks.

- Separate tasks by function and vary procedures by day and individual.
- Enforce mandatory vacation policies.
- Contact your local chamber of commerce or police department for sources of fraud prevention training.

Maintain a secure electronic environment

Maintain up-to-date systems and software, and establish policies and procedures that maintain secure passwords and security tokens.

- Establish dual controls by separating tasks of issuing and approving online payments.
- Use security tokens and secondary authorization from a separate workstation.

- Limit internet use on computers used for online banking.

Issue secure checks

Ensure your accounts are set up properly and notify your bank when changes occur relating to your check authorization.

- Notify your bank when a checking account needs to close.
- Only sign checks once the recipient and amount information is completed.

Secure check storage

Separately maintain check supplies and check producing equipment in a secure, locked facility.

- Use secure check stock with a minimum of eight security features.
- Limit access to check supplies and equipment and conduct frequent surprise audits.
- Frequently change procedures and rotate responsibilities of personnel.

Accept authorized checks

Ask for appropriate identification and use check verification services to ensure check authorization.

- Vary deposit procedures by day and individual, and review daily reports.
- Use bonded couriers to make deposits.

An example of a payments fraud prevention best practice put to work

The situation

An organization initiates ACH transactions over the internet for vendor payments and payroll direct deposit. A malware-infected workstation has detected ACH payments by capturing an employee's keystrokes. This enables the hacker to send a fraudulent ACH payment, which results in the loss of tens of thousands of dollars.

The solution

Dual controls for payment initiation and payment approval would have prevented this loss.