Tips to prevent payment fraud and cybercrimes.

Payment fraud and cybercrime are always on the rise and criminal methods are always changing.

That's why it's essential to keep up with best practices to combat them. Know what you're up against and assess your readiness using these tips. Together, we can combat illegal activity and keep accounts secure.

Prevention begins with people

- Educate and train employees at regular intervals—this is key to reducing human error
- Treat security awareness as an ongoing program, not a single project
- Create and sustain a culture that enables employees to build awareness and apply best practices
- Foster a culture that supports and rewards a "human firewall" that is proactive and pre-emptive against fraud and cybercrime
- Empower employees to report suspicious activities and enforce policies to reduce fraud risk

Check Fraud

- Use Check Positive Pay, ideally with payee verification
- Set default for exceptions to "do not pay"
- Automate check processing or outsource to reliable service providers
- Use security features on checks and secure when not in use
- Activate ACH Positive Pay for checking accounts to avoid unauthorized electronic transfers

Card Fraud

- Use Address Verification Services (AVS)
- Request CVV/CVC for Card Not Present (CNP) Transactions
- Send confirmations independent of transactions
- Process refunds only to the original card number
- PCI Compliance is required of all merchants

Electronic Payment Fraud

(includes wires and ACH)

- Activate ACH Positive Pay on all accounts, including debit blocks and filters
- Employ dual controls
- Sign up for automated alerts, same-day reporting
- Use a separate account for ACH activity only, especially payroll
- Establish templates for pre-authenticated payment instructions
- Centralize transactions in Accounts Payable to maintain a clean audit trail
- Explore UPIC technology for ACH credits

General Fraud

(regardless of payment type or fraud attack vector)

- Establish policies and procedures to identify, report, and remediate fraud and cybercrime incidents
- Use dual- or multi-factor authentication
- Segregate duties and limit access to systems or sensitive information according to job roles
- Verify payment instructions verbally with suppliers using known contact information
- Be alert to social engineering attacks such as Business Email Compromise (BEC)
- Reconcile accounts frequently, if not daily

TD Bank

America's Most Convenient Bank®