Fighting Business Financial Fraud With You

FIRST HORIZON®

Financial fraud is big business

Let’s Put Your Information on Lockdown

We understand the constant battle your business faces in safeguarding sensitive business and account information from fraud attempts. It’s not just revenue at stake, but also time working to identify and eliminate check fraud as well as maintain control over ACH and wire transactions. Fortunately, when it comes to your financial security, you’ve got a bank that has your back.

What you need

Our Solutions

Controlling Check Fraud & Forgery

Lockbox Services
Segregate the responsibilities of billing and receiving to prevent “unauthorized” internal losses. Lockbox Image Services offer you paperless workflow solutions that can provide secure, controlled access to a payer’s check or remittance documentation containing customer-sensitive data, such as credit card or patient health information.

Check Positive Pay
Combat check fraud and forgery by matching checks presented for payment against an approved list of checks issued by your business. Those without an exact match will be flagged as suspect and reported to you for a pay/no-pay decision.

Controlling Electronic Fraud

ACH Positive Pay
ACH debits to your account are compared to existing authorizations you previously set up. Items matching the criteria you establish will be released for payment. Any exception, or ACH debit without a prior authorization on file, will be available for your online review and decision.

Commercial Card
Commercial card programs can help reduce fraud exposure through electronic payments, automated spending controls, and more efficient reconciliation.

International Wire Block
Prevents the release of wired funds to any beneficiary located outside the U.S.

Complete Credit/Debit Blocks
Control both check fraud and forgery and electronic fraud by completely blocking all incoming debits and/or credits and enable full control over your account.

Benefits to Your Business

- Improved control and security with the ability to make pay/no-pay decisions on potentially fraudulent items.
- Convenient access to our tools through our secured online banking applications.
- Lower costs through reduced fraud exposure and potential losses associated with electronic payment fraud.
- Reduced work-hours resulting from items being reviewed before they travel through the banking system.

A typical business loses 5% of its revenues every year to fraud.*

That's a median annual loss of

$125,000

*Association of Certified Fraud Examiners, Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse.

Safeguards Beyond Our Solutions

Services that help protect you are great. But what about the processes and technology you use? Here are a few safeguards First Horizon Bank provides our clients to enhance their security protocols.

- **Dual Approval** – Require two separate people to approve changes to user entitlements, beneficiaries, and payment instructions.
- **Set Limits** – Establish limits for online banking transactions.
- **Security Tokens** – Users are required to enter tokens when originating ACH or wire transfer and for user administration.
- **Enhanced Encryption** – When you exchange financial data with us, you can be sure that it is encrypted using some of the highest levels of encryption available from trusted certificate authorities. When you see our name in green on your address bar, encryption is protecting your data.

We protect your data from malicious attacks against our servers using firewalls and intrusion detection systems. These solutions not only help protect our applications from hackers, but also detect intrusion attempts and alert us.

What You Can Do to Protect Yourself

- Conduct reconciliation of all banking transactions on a daily basis.
- Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Familiarize yourself with First Horizon Bank's account agreement and with your liability for fraud under the agreement.
- Stay in touch with other businesses to share information regarding suspected fraud activity.
- Immediately notify and escalate any suspicious transactions to First Horizon Bank, particularly paid checks, ACH or wire transfers. There is a limited recovery window for these transactions, and immediate notification and escalation may prevent or minimize loss.

Other General Security Practices

- Be wary of phishing email scams that attempt to gather sensitive information or deploy malware.
- Do not click on links or attachments in unknown or suspicious emails.
- Use dedicated PCs for sensitive online transactions.
- Establish a password-protected screensaver set to activate after some period of inactivity.
- Use bookmarks or saved links to access Online Banking.
- Log off and close browser windows of websites when you are finished.
- Shred sensitive data and use secure shred bins.
- Consider hiring security professionals to test your security procedures and offer training programs.
- Be cautious of emails that appear to be a vendor or customer requesting a change in payment information. Any changes requested by email should always be authenticated by performing a callback verification to the vendor/customer's telephone number on file.

You Earned It. Now Keep It.

For more information on strengthening the security of your bottom line, contact your Relationship Manager or Treasury Management Services Officer.