FIRST BANK

Fraud checklist for your business

Fraud can occur at your business at any time. That's why implementing a multi-layered approach is essential to helping protect your assets. To help reduce the risk of fraud at your business, please review this helpful list of actions you can take right away.

Internal controls and processes

- ✓ Educate personnel regularly on the importance of safeguarding sensitive information and following established procedures.
- ✓ Limit access to sensitive information (such as payment, credit card, personal information, and account information) to only necessary employees.
- ✓ Establish a retention plan for confidential information to be securely shredded or deleted off networks.
- ✓ Segregate duties when possible and have dual controls in place for initiating higher risk transactions, such as ACH, wire and account transfers.
- ✓ Establish limits at the user and company level for higher risk transactions, such as ACH and wire.
- ✓ Review employee access regularly to ensure it is accurate and remove terminated employees' access when they leave.
- ✓ Ensure internal procedures are being followed by conducting surprise audits.
- ✓ Safeguard check stock by keeping in a locked cabinet and maintain a check log to account for check numbers.
- ✓ Keep checks received from customers secure/locked up until they can be deposited
- ✓ If you have obtained ACH authorizations from clients or employees, ensure those are securely saved
- ✓ Take checks to post office to mail rather than placing in mailbox.
- ✓ Utilize bill pay and/or pay invoices online with the vendor directly or call the vendor to authorize a phone payment.
- ✓ Reconcile your books with your bank statements on a regular basis and verify the payee on checks clearing your account match who they were initially made payable to. With the increase in check fraud nationwide, fraudsters may intercept a check in the mail and change only the payee without changing any other additional information.
- ✓ Verify out of the norm payment requests/instructions from internal employees and vendors prior to the payment being initiated and sent. Business email compromise scams can consist of a fraudster using a compromised employee or vendors' email to send a new request for payment and/or routine payment request with "updated payment instructions" to a different account.

Employee training and awareness

- ✓ Provide regular training to employees on identifying, reporting, and preventing fraud.
- ✓ Test employees' understanding of fraud tactics through social engineering scenarios.
- ✓ Ensure staff understand how their role helps prevent fraud losses.

Technology tips

- ✓ Use a dedicated PC to conduct business transactions (limiting use of personal computers.)
- ✓ Update your software regularly and set updates to happen automatically if possible.
- ✓ Ensure company issued devices are equipped with anti-virus and anti-malware solutions.
- ✓ Use a hardware or software firewall.
- ✓ Complete periodic offline and off-site backups as if the primary data is compromised (such as in a ransomware situation) the offline and off-site copy of the data could be used to restore systems.
- ✓ Password protect your devices and do not leave them unattended.
- ✓ Create unique, long, complex passwords with upper and lower-case letters, numbers and special characters.
- ✓ Do not write down your passwords, instead use a password manager that secures your passwords in one location and are encrypted when not in use.
- ✓ Change passwords every 180 days.
- ✓ Use multi-factor authentication when possible as an additional layer of protection.
- ✓ Encrypt devices and forms of communication that contain sensitive information (such as payment, credit card, personal information, account information.)
- ✓ Have an incident response plan in place.
- ✓ Train employees on how to utilize technology and be cyber safe.

Utilize bank services

- ✓ For the ultimate protection against payment fraud, consider Positive Pay Plus, our mitigation solution, which includes both Check Positive Pay and ACH Positive Pay.
    - **Check Positive Pay** verifies each paper check you issue against a list you provide, paying only the ones that match.
    - **ACH Positive Pay** reviews outgoing electronic payments (ACH) against your approved list, allowing only authorized transactions to help prevent fraud.

  Contact us to learn more at **treasurymanagement@myfirst.bank**

  $40 per first account, and $30 each additional account per month, per account.

Your security is always our priority

For questions, start a chat with us in your First Bank Online Banking or Mobile App, visit your nearest branch or call 1-800-538-3979.

Get more tips at **myfirst.bank/fraud-prevention**

FIRST BANK Member FDIC