Annual Fraud Protection Checklist

FIRST first financial bank

The new year is a great time to step back and review the protections you have, or do not have, in place.

Use this checklist to evaluate your current fraud prevention strategy, and verify that your business is prepared for the coming year and its inevitable fraud attacks.

☐ Conduct an annual review of accounts, access, and systems.

Risk Scenario: *A fraudster stole a credit card linked to a former employee. Because the card wasn't closed or monitored, several small unauthorized charges accumulated to thousands of dollars. An annual review would have identified and closed the inactive card, eliminating this risk.*

☐ Update antivirus software, firewalls, and browsers, and disable unnecessary plugins or cloud access.

Risk Scenario: *A business neglected to add a critical firewall update. A hacker scanned for outdated versions, found the vulnerability, and gained access to the internal network. With this access, the fraudster had the opportunity to access sensitive account information. Had the system been updated, the security patch would have blocked the intrusion.*

☐ Assess your payment policy.

Risk Scenario: *A fraudster used a fake email address mimicking the company's internal email addresses to request a new vendor for an urgent project. Because the internal accounts payable processes are not thorough, the fake vendor was added and paid before the fraud was detected. A stronger payment policy with thorough approval and validation processes would have flagged and prevented the scam.*

☐ Consult with a third-party risk management company to identify potential vulnerabilities in your systems.

Risk Scenario: *A third-party audit discovers that an entire team uses the same password for all systems. The company uses this learning to implement new password requirements and two-factor authentication for internal systems. Before the assessment, a stolen password could have unlocked many confidential files.*

☐ Implement or reinforce dual control on company payments.

Risk Scenario: *A cyber criminal gained access to an employee's email and attempted to authorize a wire transfer. Because only one approval was required, the transfer went through. Dual control would have stopped the transaction by adding another required authorization.*

☐ Train employees to know and understand current fraud trends, such as AI deepfakes and social engineering.

Risk Scenario: *An employee joined a virtual meeting where their supposed manager requested an urgent wire transfer. Unbeknownst to the employee, the meeting's audio and video were AI-generated using public content from news and LinkedIn posts. Without proper training on verifying unusual and urgent requests, the employee processed the transfer, resulting in fraud. Proper training could have helped the employee spot red flags and follow verification protocols, preventing the loss.*

☐ Verify company payment instructions.

Risk Scenario: *A business owner received an email from a vendor with details about new wire instructions. Without verifying by phone call, the owner sends the payment. If the company had called a known, trusted number to confirm the new instructions, the company would have learned that the new wire instructions were fraudulent and could have been saved from paying a false invoice.*

☐ Consider switching to electronic payments.

Risk Scenario: *Every month, a business pays rent with a mailed check. A scammer interferes with the payment in the mail, washes the check, changes the payee, and then redeems the payment for their own uses. Electronic payment helps eliminate this physical check threat.*

☐ Verify unusual or unexpected payment requests.

Risk Scenario: *Fraudsters take over a company's CEO, CFO, or other Senior leaders' email to make it look like a payment request is coming directly from them. This is an attempt to avoid established protocols and divert funds to the bad actors. Also confirm unusual requests by reaching out to the person making the request separately using a known, trusted contact method other than email.*

☐ Take advantage of the fraud mitigation services your bank has available.

Risk Scenario: *A small business mailed a vendor a check for supplies. The fraudster stole it out of the mailbox, washed off the ink, and rewrote the check to themselves. Positive Pay would have flagged the discrepancy between the recorded intended recipient and the new fraudulent one, and often in time for the business to stop the payment.*

☐ Never share your login credentials or one-time passcodes with anyone, even if the caller claims to be your bank.

Risk Scenario: *A fraudster impersonates a bank to "confirm" a wire transfer. After obtaining the customer's login credentials and token, the fraudster gains full access and sends fraudulent wires.*

For more resources and tips, visit
www.bankatfirst.com/fraud-awareness

To report fraud, contact the Business Support Center at (866) 604-7946.
To learn more about how First Financial Bank can help our customers mitigate risk, contact your Treasury Management Advisor.