fIRST® first financial bank

2023 fraud awareness best practices

Payments fraud continues to be a significant business challenge. According to the 2022 AFP® Payments Fraud and Control Survey, in 2021 71% of organizations were victims of payments fraud attacks/attempts and 68% of organizations were targeted by a Business Email Compromise scam. If that sounds alarming to you, you're not alone. But we can help your business be more efficient in identifying potentially fraudulent transactions and equipping you with a proactive approach to protecting your accounts from unauthorized activity.

PAYMENTS

- □ Validate all change in payment instructions by calling a trusted and documented account representative - never call the number listed on the invoice or within the electronic invoice
- □ Pay by Corporate Card when possible

PROCESS

- □ Reconcile all accounts to include credit cards, as often as capable
- □ Educate your employees about email, text, Business Compromise and other scams - through consistent/ organized employee training
- □ Require dual control for all steps of cash handling, payment initiation and payment file management
- □ Employees that issue payments by check or electronically (ACH/Wires) should not also reconcile the account
- □ Implement procedures for when an employee suspects infection
- □ Report all fraud to First Financial Bank immediately - Business Support Center (866) 604-7946
- □ Never leave sensitive information on desktops or printers
- □ Use strong and unique passwords for all online account access. Avoid using the same password for various sites
- □ Keep all authorized signors and online banking Administrators updated with your bank
- □ Utilize Check Positive Pay and ACH Debit filters even on low activity accounts
- □ Do business with customers you know – be wary of 'too good to be true' business including people who want to pay upfront or pay more than cost
- □ Force vacation time of all accounting/finance staff. While away, audit that employee's activity. Be wary of employees who refuse to take vacation time.

SYSTEMS

- □ Disable CD/DVD/USB access if not essential
- □ Protect the company network by using a firewall
- □ Keep all anti-virus and anti-malware software up-to-date
- □ Keep your system patched and updated
- □ Regularly backup important data and files to a secure off-site location, and periodically test recovery to validate the process
- □ Use keycards and electronic locks whenever possible, and make sure to document who has access to physical keys