OLD NATIONAL BANK®

Fraud Prevention Checklist

Reduce Your Risk

When running a business, risks can present themselves any time—and anywhere. By being aware of the risks you can control and putting proper precautions in place to mitigate them, you can keep your focus on moving your business forward—and Old National can help.

The Basics

Employee Training

- ☐ Train employees about the proper handling of sensitive information, including account numbers, credit card information and personal information.
- ☐ Teach them how to identify common scams, including business email compromise, phishing, cyberattacks, phone scams, pop-up ads, social engineering and malicious links and attachments in emails.
- ☐ Restrict access to areas where sensitive information is stored—train employees to look out for uninvited people on premises.
- ☐ Reinforce these practices with annual refreshers.

Safeguarding of Information

- ☐ Institute a “clean desk” policy.
- ☐ Contract with a reputable document destruction company or buy cross-cut shredders.
- ☐ Create a policy for document retention and safekeeping, including destroying documents that are no longer necessary to retain.

Annual Check-Ups

- ☐ Meet with your Old National Treasury Management banker to review your online banking controls and services.
- ☐ Contact your Insurance Agent to review policy coverage, including coverage for cyber-crime and employee theft and dishonesty.

Technology

Networking

- ☐ Use business-grade modems and routers.
- ☐ Password protect wireless networks.
- ☐ If you offer guest or customer WiFi, keep it on a separate network from your business devices.

Software

- ☐ Keep your operating system up to date.
- ☐ Install and regularly update anti-virus, firewalls, anti-malware and anti-spyware software.
- ☐ Add external email alerts to your email software.
- ☐ Regularly back up your hard drives in a secure fashion.
- ☐ Keep web browsers and other software (Java™, Adobe, etc.) updated.

Hardware

- ☐ Use a dedicated computer for online banking activities that is segregated from your network.
- ☐ Restrict use of removable storage devices (USB flash drives, external hard drives, etc.)

Passwords

- ☐ Password protect computers and mobile devices. Lock devices before walking away.
- ☐ Use unique passwords whenever possible.
- ☐ Create long, complex passwords with upper and lower-case letters, numbers and special characters.
- ☐ Never share or write down your password.
- ☐ Change passwords at least every 60 days.
- ☐ Use two-factor authentication when available.

Fraud Prevention Checklist

Controls & Processes

Review Access Permissions

- ☐ Review who has access to your computer network and systems on a scheduled basis (at minimum, quarterly).
- ☐ Audit employee permissions to ensure proper safeguards are in place.

Transaction Controls

- ☐ Set controls for high-dollar transactions.
- ☐ Require multiple users to approve transactions above a defined amount.
- ☐ Use Positive Pay services to control for unauthorized or fraudulent check and ACH items.
- ☐ Perform call-backs for email payment requests or changes to on-file payment information.

Manage Document Retention

- ☐ Secure sensitive information, including remotely deposited checks, bank statements, credit card statements, sensitive employee information, etc.
- ☐ Document where sensitive documents are housed and who can access them.
- ☐ Shred or destroy items after they are no longer useful.

Create & Test Procedures

- ☐ Create a documented plan for various scenarios - natural disasters, power outages, pandemics, etc.
- ☐ Know who is responsible for what and when.
- ☐ Test your plans (at minimum, annually).

Use Bank Services

Add Fraud Prevention Services

- ☐ Check Positive Pay lets you review in-clearing checks, returning those that are unauthorized or altered.
- ☐ ACH Positive Pay allows pre-authorized items to post, allowing you to review and return new or unexpected items.
- ☐ Add Encryption & Tokenization services to your card terminals to help protect your payment data.

Send Payments Electronically

- ☐ Subscribe to online wire transfers to leverage automatic controls.
- ☐ Convert check payments to ACH or wires to reduce risk of checking account compromise.

Add Dual Controls

- ☐ ACH, wire transfers and account transfers have optional dual approvals.
- ☐ Restrict online banking permissions to allow certain users to maintain payees and others to initiate payments.

Segregate Duties

- ☐ Reconcile your account often—daily, if possible—with the responsibility rotating between employees.
- ☐ Outsource your mail opening to a Lockbox, adding a layer of control to your business.
- ☐ Subscribe to Account Reconciliation services, where the bank completes an independent balancing of your account.

Old National Can Help

Old National Business Security Center: oldnational.com/security/business-resources

Old National Treasury Client Services: 800-844-1720 or treasurymanagement.customerservice@oldnational.com

2329900-0923-109