

Fraud Prevention Checklist

Use this checklist to review your fraud prevention procedures and ensure that you have all of the controls in place to protect your organization's future.

We recommend you review this information on a semi-annual basis.



CHECK SUPPLY

- **Carefully choose your check vendor.** Use an established, respected provider.
- **Limit check styles.** Using one style of checks for each account will allow for easy recognition.
- **Security.** Incorporate security features into the check design.
- **Monitor supply shipments.** Notify your supplier if check orders are not received within a reasonable time.
- **Utilize secure storage areas.** Store blank checks and check printing equipment in a secure area with controlled access. Then, limit the number of checks removed from the secure area.

FRAUD PREVENTION SERVICES AND TOOLS FOR TRANSACTIONS

Paper-based transactions:

- Positive pay
- Block check writing activity
- Elect check safekeeping and truncate your accounts

Electronic transactions:

- Debit blocks—keeps all ACH originators from debiting your account
- Debit filters—set who can access your account (cannot limit amounts)

All transactions:

- Utilize Online Banking to review account daily
- Reconcile daily/monthly (including separation of duties between who issues payment versus who reconciles)

ONLINE FRAUD PREVENTION

- **Virus protection software.** Install on all computers and schedule updates at least daily.
- **Separate controls for your business Online Banking.** Use one computer to create online payments; have a second user approve those payments from a different computer.
- **Limit Internet use on computers used for Online Banking.** This reduces the risk that malicious programs will infect those computers.
- **Monitor account balances and activity daily.** Report any suspicious activity immediately by calling customer service or your banker.
- **Consider the use of anti-spyware application as well as a firewall.** Schedule updates frequently.
- **Check your operating system on a regular basis.** Install all the latest patches and updates.

- **Only apply updates from trusted sites.** Beware of download requests from pop-ups or advertisements.
- **Avoid using e-mail to send confidential information.** If you must send sensitive information, mask out all but the last four digits of your account number.
- **Review all e-mail from the bank.** You will receive e-mail messages automatically when your challenge questions are answered correctly, as well as when ACH or wire transfers are processed. You must notify the bank immediately if you receive such an e-mail and the user has not logged in or submitted any such ACH or wire transfers to the bank.
- **Account shut down notices.** If you receive an e-mail that warns you, sometimes with little or no notice, that your account will be shut down unless you confirm your billing information, do not reply to the e-mail, or click on any links in the e-mail; instead, you must contact the company referenced in the e-mail by telephone or by using a website address that you know to be genuine.

PROCEDURES

- **Dual control.** Implement dual control procedures with the following transactions: Web ACH, Remote Deposit, Wires, and Check Automation.
- **Transaction Review.** Review transactions before they leave the company.
- **Conduct surprise audits.**

CONTROLS

- **Limit Authorizations.** Only give financial access to employees who need it.
- **Do not share IDs or passwords.**
- **Preauthorize high value checks.** Approve large amounts before checks are written.
- **Never sign checks in advance.** Only sign after the recipient and amount information have been entered.
- **Signature cards.** Review and update bank signature cards annually.
- **Clear division of duties within your accounting department.** Give accounts receivable access to send receivables and post receivables. Give accounts payable access to check writing and reconciliation.
- **Review employee access privileges regularly.** If employee transfers to a new department or position within the company, review what systems the individual has access to.
- **Review your annual report.** If you have included executive signatures, consider removing them to prevent someone from illegally scanning and using.

I acknowledge that Northwestern Bank 1) has reviewed this Fraud Prevention Checklist with me, 2) has provided me with a copy for my records, and 3) has recommended that I use these tools and procedures to protect myself and my business.

Customer Signature

Date

Print Name