WINTRUST
TREASURY MANAGEMENT

wintrust.com/security

# FRAUD PROTECTION CHECKLIST

Reports of fraud are rising, and criminals continue to take advantage of businesses. Consider the following to safeguard your business from fraudulent attacks. If you have any questions or need assistance, please contact your banker or treasury management services sales officer.

## Fraud Prevention Red Flags

**Texting/Telephone/Fake Caller ID Scams**

If you receive a telephone call or text from "Wintrust Community Bank," "Wintrust Community," or anyone claiming they are from the bank asking you for your account number, password, or mobile banking login information, or if they ask you to download software or an app to your device that can access your bank account, THEY ARE A CRIMINAL — NOT A BANK EMPLOYEE. With the rise of Caller ID fraud, it's paramount to know you are talking to a REAL Wintrust banker at a Wintrust Community Banks branch.

A real bank employee already has access to your bank account information, so they would NEVER ask you for this information over the phone or need to download an app to view it.

Criminals often use a technique called "spoofing," which involves masquerading as a bank when calling customers. If you receive a call or text from someone claiming to work for a bank and it feels off...

- Delete the text/hang up the call immediately.
- Contact your banker directly via a trusted phone number or by visiting your local bank branch.

**Payment Scams**

When sending payments, ALWAYS verify payment instructions verbally before sending a wire, ACH, or Zelle® payment[1]. Faster payments mean faster fraud; don't let anyone rush you.

## What To Do if Fraud Occurs

- ☐ Provide your bank with a report of all outstanding checks/electronic transactions that must be honored.
- ☐ Log the fraud with the FBI at ic3.gov, even if a loss is not incurred. The more detail you enter, the more beneficial it is to them; they use victim reports to determine if the perpetrator has other victims and help develop a case against the criminal.
- ☐ Complete the Affidavit of Forged Signature/Endorsement or the Affidavit of Alteration Form provided by your banker.
- ☐ You should file a police report at your business's local police station and provide fraudulent check images when filing.
- ☐ Add appropriate fraud prevention services, such as Positive Pay products (ACH, check, or payee Positive Pay), or close the account and open a new account. Action needs to be taken as soon as possible to avoid further fraud, and we highly encourage adding fraud prevention services on all transactional accounts as a preventative measure.
- ☐ Contact your business insurance provider to review the current policy coverage and verify if they have cybersecurity insurance.

**1. Zelle®.** Zelle® is intended for sending money to people and businesses you trust. Dollar & frequency limits apply. Transactions between enrolled consumers/users typically occur in minutes. To send or receive money with Zelle®, both parties must have an eligible checking or savings account.

## Information Security

- [ ] Do you have an information technology (IT) manager?
- [ ] Do you have a policy that addresses information security?
- [ ] Is your workplace secured with an alarm system or do you have access controls?
- [ ] Do you maintain an internet firewall?
- [ ] Do you use and regularly update anti-virus software?
- [ ] Are your computer systems and equipment configured to install critical security patches automatically when they are released?
- [ ] If you use a wireless network, is it secure, and are transmissions encrypted?
- [ ] Are access controls in place for computer and information systems with multiple users, restricting access based on a user's need to know? Is access defaulted to "deny all" unless an exception is granted?
- [ ] Do you have a change management policy in place to revoke user access to systems when necessary?
- [ ] Are computer and network passwords changed at least every 90 days?

## Bank Reconciliations

- [ ] Are all items on your bank account statement reconciled and accounted for monthly?
- [ ] Are bank reconciliations reviewed for canceled checks and unusual items?
- [ ] Are all images of checks reviewed for any possible alterations?
- [ ] Are bank reconciliations reviewed and adjustments to the cash accounts approved by you to underline dual control?
- [ ] Do you review cleared checks and ACH items for missing numbers, out-of-sequence numbers, or fraud?
- [ ] Are all checks recorded as they are issued?

## Accounts Receivable and Accounts Payable Controls

- [ ] Are accounts receivable aging lists reviewed?
- [ ] Are all sales orders recorded on pre-numbered forms? Are all numbers accounted for?
- [ ] Are monthly statements reviewed for outstanding balances?
- [ ] Are checks to vendors matched against the invoice and proof of receipt?
- [ ] Are regular outside audits conducted?
- [ ] Is payroll processed internally or outsourced? If processed internally, is it managed under dual control?
- [ ] Are supporting documents (invoices, reports, purchase orders, etc.) presented to you with the payables checks and reviewed by you prior to signing the checks or approving ACH credit issuance?
- [ ] Are supporting documents for payables checks properly canceled to avoid duplicate payment?
- [ ] Are checks payable to cash prohibited?
- [ ] Is signing blank checks prohibited?
- [ ] Are signed checks mailed by someone other than the person who writes the checks?
- [ ] Are outgoing payables checks securely delivered to the post office rather than left for pick up?

## Cash Receipts

- [ ] Are detailed cash receipts prepared before giving them to the bookkeeper?
- [ ] Are daily detailed cash receipts compared with the cash receipts journal, duplicate deposit slip, and bank statement?
- [ ] Are cash sales controlled by cash registers or pre-numbered cash receipt forms?
- [ ] Is cash counted under dual control?
- [ ] Are cash receipts deposited daily and promptly posted to the appropriate journals?

## Check Stock

- [ ] Are all authorized signers reviewed periodically for accuracy?
- [ ] Are checks always pre-numbered?
- [ ] Is the check stock kept in a secure location?
- [ ] Do you use security protection measures on your check stock as a precaution against fraud?
- [ ] If a facsimile signature stamp is used, is it only under your sole control? Do you use it only when necessary rather than as the norm?
- [ ] Are voided checks retained, noted, and then shredded?

## Electronic Banking

- [ ] Do you have complete access to online banking?
- [ ] Are you signed up for e-statements?
- [ ] Do you or a trusted administrator safeguard and monitor who can access the system?
- [ ] Does your network administrator require complex passwords?
- [ ] Do you regularly review online account activity, including ACH transactions and wire transfers?
- [ ] Do you have a change management policy to revoke user access to the system when necessary?
- [ ] Do you use Positive Pay to issue checks and block and filter electronic entries?

## ACH Origination

- [ ] If you utilize ACH transactions or wire transfers, is there a second level of approval on all outgoing fund transfers?
- [ ] Have you obtained signed authorizations for all accounts to which you are sending ACH debits and ACH credits?
- [ ] Are ACH debit and ACH credit authorizations maintained in a secure environment with access limited to authorized personnel?
- [ ] Are ACH authorizations retained for at least two years from the date of the last transmission?
- [ ] Do you shred sensitive information documents at the end of the retention time?
- [ ] Do you review ACH origination entries and templates regularly?
- [ ] Do you verify any changes to vendor banking information with a trusted source?

## Remote Deposit Capture

- [ ] Do you retain original scanned checks for at least 30 days but not more than 60 days?
- [ ] Do you retain all information regarding the digitization of checks created by the system for at least seven years?
- [ ] Do you secure checks and other documents with sensitive information to protect nonpublic personal information from being compromised?
- [ ] Do you use the electronic endorsement feature of check scanning? If so, are the endorsement settings for each account correct?
- [ ] Are all scanned checks made payable to the account holder of record as shown on the bank statements?
- [ ] Are all remote deposit checks endorsed to avoid duplicate deposits?

## Miscellaneous

- [ ] Are annual one-week vacations mandatory for all employees with access to books, cash, or receivables duties?
- [ ] Are employees cross-trained so no one individual is always responsible for a specific duty without oversight?
- [ ] Have there been any changes in management or the responsibilities of key employees that should be communicated to the bank?
- [ ] Do you have a training program for employees about cybersecurity and social engineering?
- [ ] Do you have a fraud disaster recovery plan?

*Last updated 8/2025.*