



Mercantile Bank is committed to maintaining your security and privacy while helping you bank the way you want. Your privacy is considered in all aspects of our business. We use industry standard security techniques to ensure your personal financial information remains confidential, and we limit the sharing of your information to the necessary data needed to conduct business, provide quality service, and offer other products and services that would meet your needs.

Protecting Yourself and Your Funds

Mercantile Bank Fraud Prevention Efforts

Corporate Loss Prevention utilizes a suite of fraud prevention software tools that monitor customer accounts on a daily basis for a variety of possible fraudulent activities; however, it is your responsibility to ensure that your computer systems and online credentials are properly secured. Not following the basic precautions referenced in this document exposes you and your systems to significant risk.

If a fraud is detected, we work closely with your branch personnel to ensure that not only are you contacted, but that you are assisted in the various steps needed to resolve the fraud situation.

General Fraud Prevention Tips

- Monitor your accounts on a daily basis.
- Delete all unsolicited e-mails from work computers.
- Check bank statements immediately when they are received and report any unauthorized activity immediately.
- Maintain applicable accounts/records under dual control; never let one person have sole access to records or accounts without a second person approving and reviewing files before uploading.
- Take all outgoing company mail to a secure mailbox.
- Shred unwanted documents that contain sensitive information before disposing of them, including junk mail, financial solicitations, bank statements, paid checks, doctor bills, and insurance documents.
- Use a lockbox if you receive customer payments after business hours.
- Dual control and segregation of financial responsibilities should be utilized even in smaller companies.

Tips for Preventing Internet Fraud

- Utilize virus protection software and firewalls.
- Keep computer software updated and current.
- Use strong passwords (mixture of alphanumeric characters with both upper and lower case used).
- Ensure you have a secured link on your browser (lock symbol at the bottom of the browser) before entering password information.
- Never give your username and password to anyone. Do not write this information down.
- Manually change passwords on a regular basis or set software settings to automatically prompt for regular password changes.

This document provides a basic overview of fraud/risk management recommendations and is not intended to be used as legal advice. There is no warranty, expressed or implied, in connection with making this information available.

Mercantile Bank Fraud Prevention Efforts

Tips for Preventing Card Fraud

- Keep a list of all your credit cards and bank accounts along with their account numbers, expiration dates and credit limits, as well as their respective fraud department phone numbers in a safe place.
- Never give company account numbers or credit information to anyone you don't know.
- Remember that we will NEVER call to ask for account or personal information.
- Keep an updated list of which employees have company credit, debit, or ATM cards, along with account numbers, expiration dates, and limits.
- Keep track of card receipts. Ask that they be submitted for any expense reimbursements.
- Cancel and destroy any unused cards.

Tips for Preventing Check Fraud

- Implement positive pay. It's the most effective way to identify check fraud.
- Safeguard incoming and outgoing mail. If regular statements or bills fail to reach you, call the company to find out why. Put outgoing mail in a secure mailbox.
- Reconcile monthly statements ASAP. Report questionable activity immediately to prevent any additional fraud.
- Perform research before giving checks to any unfamiliar charities or organizations.
- Pay bills online to reduce your check volume in circulation.
- Bank accounts should be reconciled by someone other than the person issuing checks, making deposits, performing transactions.

Safeguarding Customer Information

Mercantile Bank uses industry standard security techniques to ensure your personal financial information remains confidential.

Mercantile Bank limits the sharing of your information to the necessary data needed to conduct business, provide quality service, and offer other products and services that would meet your needs.

We are committed to protecting the confidentiality of customer information. Your privacy is considered in all aspects of our business. As such, we maintain physical, electronic, and procedural safeguards to protect customer information. We restrict access to customer information to only those employees with a business reason to know such information. All employees are bound by a code of ethics to protect the confidentiality of customer information and are trained to maintain a high level of confidentiality.

We do not share your information with third party vendors other than those acting on our behalf to process your banking information, and they are contractually obligated to maintain information security safeguards. We may disclose customer information to other types of non-affiliated third parties such as retailers, nonprofit organizations, travel companies, and membership organizations, unless you have directed us not to do so.

Report Identity Theft If you believe you have been the victim of identity theft or fraudulent e-mail, call us toll-free at 866.345.9270.