How to Protect Yourself

General Fraud Prevention Best Practices

- Carry only necessary information with you. Leave your social security card and unused credits cards at home in a safe and secure location.
- Make photocopies of vital information you carry regularly and store them in a secure place.
- Do not provide your tax identification number or social security number unless absolutely necessary.
- Replace paper invoices, statements and checks with electronic versions, if offered by your employer, bank, utility provider or other third party vendor.
- If you have online account access with Farmers & Merchants State Bank, you can reduce paper statements (and the potential for ID theft) by signing up for Bill Pay and free electronic statements.
- Shred documents containing business, personal or financial information before discarding. Most fraud and identity theft incidents happen as a result of mail and garbage theft.
- Review your credit report at least once a year, looking for suspicious or unknown transactions. You can get a free credit report once a year from each of the three major credit bureaus at www.annualcreditreport.com. For a small fee you can obtain a copy at any time directly from:
    - Equifax: 1-800-685-1111 or www.equifax.com
    - Experian: 1-888-397-3742 or www.experian.com
    - TransUnion: 1-800-916-8800 or www.transunion.com
- Subscribe to a daily **credit monitoring service**, such as Farmers & Merchants State Bank Bank's ID Theft Protection (this applies to consumers only and other restrictions apply; refer to terms and conditions.)
- Place outgoing mail in a U.S. Postal Service mailbox to reduce the chance of mail theft.
- Promptly retrieve incoming mail to limit the opportunity for theft.
- Know your billing and statement cycles. Contact your vendor’s customer service department if you stop receiving your regular bill or statement.

If you think you are a victim of fraud:

- Immediately cease all activity from computer systems that may be compromised. Unplug the Ethernet or cable modem connection to isolate the system.
- Immediately contact Farmers & Merchants State Bank so that the following actions may be taken as a priority to contain the incident:
    - Online access to the accounts be disabled.
    - Online account passwords changed.
    - New account(s) opened as appropriate.
- Review all recent transactions and electronic authorizations on the account.
- Ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address.
- File a police report with the local police department and provide the facts and circumstances surrounding the loss. Obtain a police report number with the date, time, department, location and officer’s name taking the report or involved in the

subsequent investigation. Having a police report on file will often facilitate dealing with insurance companies, banks, and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.

- Maintain a written chronology of what happened, what was lost and the steps that you took to report the incident to the various agencies, banks and firms impacted.
- Record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.
- Review the recommendations at the Federal Trade Commission's Identity Theft website.
- Consider hiring a consultant to have your network and systems reviewed by a qualified computer forensic/information security professional.

Online Security Best Practices

- Use a current web browser.
- Clear the web browser cache before you begin an online banking session.
- Avoid using automatic login features.
- Create strong passwords with at least 10 characters, including lower-case and upper-case letters, numbers and special characters.
- Don't use Personally Identifiable Information (PII) as a username or password, such as your social security number.
- Change your usernames and passwords regularly.
- Avoid using the same username and password on your online accounts.
- Protect your username and password – don't write them down and don't share them with others.
- Protect your answers to security questions – don't write them down and don't share them with others. Select questions and provide answers that are easy for you to remember, but hard for others to guess.
- Avoid using the same security questions on your online accounts.
- Check online banking account balances and activity daily and immediately notify Farmers & Merchants State Bank of any suspicious activity while accessing online services.
- Don't access online services from public computers, kiosks, etc.
- Never leave a computer unattended while using any online service.
- Shop with online merchants that you know and trust. Ensure that online purchases are secured with encryption to protect your information. Look for secure transaction symbols such as a lock symbol in the lower right corner of your web browser, or https: in the address bar of the website.
- Always log off from a website after making an online purchase. If you cannot log off, close the web browser completely to prevent unauthorized access to your information.

Computer Security Best Practices

- Keep your computer operating system and computer applications up to date to ensure the highest level of protection. Apply the latest patches particularly when and if they apply to a known exploitable vulnerability.
- Install firewalls, commercial virus protection and spyware protection and keep them up to date to ensure the highest level of protection
- Avoid downloading programs from unknown sources
- Limit administrative rights on computers to help prevent inadvertent downloading of malware
- Turn your computer off completely when you are finished using it.

Email Security Best Practices

- Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders. Farmers & Merchants State Bank will never ask you for your password or your answers to your security questions via email.
- Immediately notify your Farmers & Merchants State Bank representative of any suspicious emails purporting to be from Farmers & Merchants State Bank.
- Always encrypt emails that contain sensitive information.

Mobile Security Best Practices

- Never disclose sensitive information via text message.
- Download mobile apps from reputable sources only and update and maintain them with the latest patches, particularly when and if they apply to a known exploitable vulnerability.
- Frequently delete messages from your device, and especially before loaning out, discarding, or selling your mobile device.
- Use the keypad lock or phone lock function on your mobile device when it is not in use.
- Always store your mobile device in a secure location.
- Immediately notify your mobile device provider if it is lost or stolen.

Scam Prevention Best Practices

- First and foremost, use common sense. If it sounds too good to be true, it probably is.
- Never give personal information to a stranger who contacts you, whether by telephone, email, or other means.
- You are responsible and liable for items you cash or deposit into your account, whether they are a check, money order, transfer, etc.
    - Don’t accept payments for more than the amount of the service with the expectation that you send the buyer the difference.

    - Don’t accept checks from individuals you’ve only met online.
    - Don’t accept jobs in which you are paid or receive commission for facilitating money transfers through your account.
- Be wary of offers of mortgage modification, foreclosure rescue, or short sale scams involving money-back guarantees, title transfers, up-front fees, or high pressure sales tactics.
- No matter how urgent someone claims a deal or job offer is, you should research and confirm its legitimacy.

Scam examples:

Job Scams: You accept a job in which you are paid to receive a commission to facilitate money transfers through your account or apply for a job that asks you to set up a new bank account. Job scammers use reputable online job boards to offer work-at-home jobs or accounting positions. These job scams may require employees to receive money into their existing bank account (or open new accounts) and then transfer the money to another account, often overseas. As payment, the job seeker is instructed to keep a small percentage of the transfer.

Lottery or sweepstakes scams: You receive notice that you are the winner of a lottery that you did not enter, but must pay a small percentage for fake taxes or other fees before you can receive the rest of your prize.

Dating scams: Someone you met through an online dating site or chat room asks you to send money for a variety of reasons, including a need for urgent surgery or to make travel arrangements to meet in person.

Internet scams: You receive a check for something you sold over the internet, but the amount of the check is more than the selling price. You are instructed to deposit the check, but send back the difference in cash.

OR

You receive a check from a business or individual different from the person buying your item or product.

OR

You are instructed to transfer money, or receive a transfer of money, as soon as possible.

Telephone scams: Unless you initiated the contact, do not give out personal information over the telephone. If the call is not initiated by you, always ask for a call-back number. Use legitimate sources to verify Farmers & Merchants State Bank contact information, including:

- www.fandmstbk.com
- Phone numbers:
    - 920-478-2181 Farmers & Merchants State Bank - Waterloo
    - 608-655-3451 Farmers & Merchants State Bank - Marshall
- Official contact information on your statements

- Phone numbers listed on your ATM, or debit card
- The security of your accounts and personal information is one of Farmers & Merchants State Bank's top priorities. We promptly investigate any reported suspicious activity.

Report Suspicious Activity

Call Farmers & Merchants State Bank immediately if you notice suspicious activity related to your investment, retirement, credit card, deposit or loan accounts.	• **Lost or stolen checks /ATM Cards:** 1-920-478-2181 • **Lost or stolen debit cards:** 1-800-383-8000 • **Suspicious online transactions:** 1-920-478-2181
Monitor your accounts regularly.	Regularly reviewing your account activity is one of the best ways to notice and stop fraudulent activity quickly. Review your monthly statements or review activity online, 24 hours a day, with Farmers & Merchants State Bank online access to your deposit, loan, retirement, and investment accounts. You can take action to protect your identity and your personal information. Contact us to sign up for ID TheftSmart™ or ID TheftSmart™ with Credit Monitoring to keep your online and offline transactions secure.