Securing Financial Information – Internet Fraud

Farmers & Merchants Bank wants you to be familiar with various forms of fraud that, unfortunately, are occurring in rising numbers. You may have heard of some types of fraud such as identity theft, check scams and Phishing. But there are a variety of frauds you should be aware of, so that you can better protect yourself and your assets. We encourage you to use caution when providing confidential information, regardless of the medium. The following are broad categories of types of fraud, as well as more specific examples of fraud you may encounter, and ways to protect yourself from such crimes and prevent becoming an uninformed victim.

Identity Theft

Identity theft occurs when scammers capture and use one or more parts of a person's identity. These can include Social Security Number, account numbers, addresses, date of birth, driver's license numbers or other pertinent information. The criminal then tries to assume that person's identity and create new accounts or gain control of legitimate existing accounts. The best way to protect yourself from identity theft is to limit the spread of your confidential information. Shred or destroy any documents that contain sensitive data before you discard them, and be aware of to whom you give such information.

Online Frauds

Phishing and Pharming

"Phishing" is a common fraud scheme whereby a customer receives an e-mail that appears to be from the Bank requesting account or personal information. Be wary of any such communication, as it is often the first step a criminal will take to commit identity theft.

"Pharming" occurs when a website redirects you to a fraudulent website without your knowledge. This website often attempts to look similar to a legitimate website, in order to trick you into entering personal information. This information can then be sold between criminals and used to commit identity theft.

Remember, in no event will Farmers & Merchants Bank ever request sensitive information from you by e-mail. Always check to make sure when logging into FMB's Internet Banking Site "WebBanker" that you are using the authentic website, (located at: http://www.fmbbank.com/), and not a look-alike site attempting to deceive you.

General Fraud

Credit Card Fraud

This fraud occurs when someone steals your credit card or card number without your knowledge or consent and uses it to conduct fraudulent transactions.

Check Scams

This scam frequently occurs during an internet auction purchase. In this scam, a counterfeit check is sent by the buyer in an amount higher than the price negotiated for purchase, and the buyer will then request the difference be wired back before the check is discovered as counterfeit. Any money you send will be lost, as the counterfeit check is worthless and uncollectable.

Phone Solicitations

Scammers can randomly call telephone numbers, with the hope that individuals will be fooled into giving private information to the caller. Sometimes, the scammer will offer prizes or rewards for divulging this information. You are encouraged not to divulge your information, as doing so can compromise your identity.

If you call Farmers & Merchants Bank requesting information about your account, we will ask you for information contained in your account records to protect your account information and identify you as authorized to receive account information. **However, in no event will Farmers & Merchants Bank ever initiate a call to you requesting your personal account information.**

Mail Fraud

Mail fraud can occur when a criminal intercepts mail intended for you and misuses information contained in the mail to their advantage. This may be the first step a criminal takes to commit identity theft. This fraud can also occur when you receive offers which are "too good to be true", a good sign that they are fraudulent.

Examples of Fraud

Below are additional examples of fraud which you may encounter. By becoming aware of how scammers operate, you can better protect your confidential information and prevent becoming a victim.

Notification of Changed Online Account Information

This scam begins with an e-mail to you requesting you to confirm that you have made changes to your online banking information, such as e-mail address or password. It asks that you click a link and verify you initiated this change. Do not click the provided link, as it will likely take you to a fraudulent webpage designed to look like the official Bank page. Instead, notify Farmers & Merchants Bank of this fraud attempt. Only access online banking through the link provided at http://www.fmbbank.com/ to ensure you are logging in to Farmers & Merchants Bank, and not a scam website. Should you suspect this scam, please notify us by phone at (850) 997-2591 or e-mail us at websecurity@fmbbank.com

Request to update your Online Account Information

You may receive an e-mail purporting to be from the Bank requesting you update account information by way of an included link. This is another example of online fraud attempting to look like official Bank communication. Again, do not click this link,

instead, immediately report it to Farmers & Merchants Bank at (850) 997-2591 or at websecurity@fmbbank.com

Veteran's Administration

The Veteran's Administration has announced the theft of information such as Social Security numbers, and date of birth, on 26 million veterans. If you are a veteran concerned about this theft, consider putting a "fraud alert" on your credit file, and monitor your credit report regularly. Following these steps will make it more difficult for a criminal to be approved for credit in your name. You can obtain a free copy of your report from each of the 3 credit reporting agencies by visiting http://www.annualcreditreport.com Should you need to file a "fraud alert", the 3 credit reporting agencies can be reached at their individual websites and phone numbers:

Equifax: http://www.equifax.com/ or by phone at 1-800-685-1111
Experian: http://www.experian.com/ or by phone at 1-888-397 3742
TransUnion: http://www.transunion.com/ or by phone at 1-877-322-8228

Counterfeit Cashier's Check Scam

You may receive a request to send a "MoneyGram" to a provided address and a cashier's check to cover the expense for more than the amount requested. An enclosed letter will direct you to send the "MoneyGram" and then deposit the check, keeping the additional amount. The cashier's check is **counterfeit**, and any money you send will be lost.

IRS Scam

The Internal Revenue Service has issued an alert pertaining to a fraudulent e-mail taxpayers are receiving. This communication may reference an additional refund or threaten an audit. Should the IRS need to contact you, it will do so by phone or postal mail, the IRS does not communicate with taxpayers by e-mail.

Sweepstakes/Lottery Scam

Various scams have been detected recently involving international lottery organizations. You may receive a notice that you have won a large cash sum and need to send a small "processing fee" to receive your winnings. **This is a scam and should be ignored.** Be wary of these notices, especially if you have not entered the lottery being referenced. Any money sent will be lost.

Phone Solicitations

At no time will FMB initiate a call to you requesting your account or personal information. Should you receive such a call, this is an attempted fraud, do not give any personal or financial information out over the telephone, keep your information private, and call us immediately at (850)997-2591 to verify the call or report the fraud.

How to protect yourself

There are many steps you can take to protect both your personal and account information. Here are a few tips to follow:

Online Fraud Attempts

- Change passwords often, and make sure the passwords you use are secure. The best passwords contain a combination of numbers, letters and symbols.
- Always type in web addresses yourself. Never click a link in an e-mail for convenience, it could lead to a website masquerading as an official website with the intent to defraud you
- Scammers may steal official logos, slogans, or even names of important Bank officers from our website in an attempt to fool you into believing you are at an official Farmers & Merchants Bank website. Always verify the website you are in before entering confidential information.

Identity Theft

- Review your credit report annually
- Shred any mail before disposing of it
- Do not include your Social Security number or Driver's License number on sensitive documents
- Do not respond to unsolicited requests for your private information.

Offline Fraud Attempts

- Memorize your pin, never leave it with your card
- Report a lost or stolen card immediately by contacting the card issuer.
- When discarding statements, bills or receipts, always shred or otherwise destroy them.
- Consider writing "check id" as your signature on your credit card, to insure your identity is verified during all transactions
- Keep a list of your cards, account numbers, and contact information in a secure place away from your wallet or purse. This will make contacting the appropriate people easier in the event it is lost or stolen.

Miscellaneous Fraud Attempts

- Use caution when giving any personal information over the phone. Always be sure you are certain you are dealing with an authorized caller and not a scammer.
- Be wary of fake check scams that offer money for little or no effort, or for depositing checks from foreign countries.
- Report lost or stolen checks immediately. Simply call (850) 997-2591
- Should you receive calls or letters concerning a loan you did not apply for, notify the lender immediately. This is a sign of possible identity theft.

Farmers & Merchants Bank is concerned about the security of your confidential information. We will **never** send an e-mail requesting confidential information of any kind. Please alert us should you receive a message of this type, so that we may properly

investigate the fraud attempt. You may do so by phone by calling (850)997-2591 or by e-mail at websecurity@fmbbank.com

For more specific and detailed information, visit these relevant sites:

OnGuard Online: Valuable tips from numerous Federal agencies to help you stay on guard against internet fraud, and protect your personal information - http://onguardonline.gov/index.html

City of Tallahassee Identity Theft Site: A one-stop resource for prevention tips, warning signs, and a list of relevant contacts for victims of identity theft – http://www.talgov.com/tpd/idtheft.cfm

Internet Crime Complaint Center (IC3): A partnership between the Federal Bureau of Investigation and the National White Collar Crime Center which accepts complaints for all types of internet fraud: http://ic3.gov

Credit Reporting Agencies: If you have been a victim of a fraud, you can place a "fraud alert" on your credit file at the following sites
Equifax: http://www.equifax.com/
Experian: http://www.experian.com/
TransUnion: http://www.transunion.com/

Annual Credit Report: You may obtain a free copy of your credit report once a year from each of the 3 reporting agencies at this website – http://www.annualcreditreport.com

Georgia Bureau of Investigation: Provides a list of helpful links for Georgia residents to guard against identity theft and fraud - http://www.state.ga.us/gbi/index.html