



**Community First bank**  
of the Heartland

## Identity Theft Awareness

Identity theft involves acquiring key pieces of your identifiable information, such as your name, address, date of birth, social security number, or mother's maiden name in order to commit fraud. With this information, a thief can do such things as take over your financial accounts, open new bank accounts, purchase automobiles, apply for loans, credit cards, and social security benefits, rent apartments, and establish services with utility and phone companies.

### Ways Identity Thieves Can Acquire Your Information

- stealing** your wallet, purse or checkbook
- removing mail** from your mailbox, either incoming or outgoing
- dumpster diving** - going through your trash
- phishing** – obtaining information by email scams or fraudulent websites
- hacking** – illegally gaining access to computer systems containing personal or financial data
- pretext calling** – using false pretenses to obtain information via telephone

### More on Phishing

When consumers receive emails requesting updated billing or personal information that seems legitimate, often it isn't. Some emails are designed to trick you into revealing your private information, such as your social security number, bank account number, or debit card number. This practice is known as "phishing".

To make these emails seem more realistic, the "phisher" often disguises himself under the logo of a known company or under the name of a trusted source such as the FDIC, a bank or an internet service provider.

If you get an email that warns you one of your accounts will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead report the suspicious activity to the company where you maintain the account and the Federal Trade Commission immediately at 1-877-ID-THEFT.

Next, review and verify credit card and bank statements as soon as you receive them. Report any suspicious activity through the Federal Trade Commission website [www.consumer.gov](http://www.consumer.gov) or call 1-877-ID-THEFT. Internet fraud complaints can be filed with the FBI.

### How to Protect Yourself from Identity Theft

Two key areas to protect yourself from Identity Theft are:

#### Protect your phone

-Don't give out financial information or other personal information such as your social security number over the telephone unless you initiated the call and you know with whom you are dealing.

-If you receive any telephone inquiries, such as asking you to confirm or verify your bank account information, contact the bank and speak with an employee to confirm that the call is legitimate.

-To prohibit telemarketers from calling you, register your home and cell phone numbers with the Federal Do Not Call Registry by calling 1-888-382-1222 or [www.donotcall.gov](http://www.donotcall.gov).

#### Protect your Personal Information

-Never routinely carry important documents such as social security cards, passports, or birth certificates in your purse or wallet. Keep important documents in a safe place at home or in a safe deposit box at the bank. Only carry them when you need them.

-Don't write your personal identification numbers (PIN) down. Instead, memorize them. Refrain from printing your social security number or credit card numbers on your checks.

-Promptly notify the bank and other creditors when you have a change of address. Contact creditors if your regular monthly or quarterly bills do not arrive when expected.

-Shred any receipts, financial statements, documents, bank statements and credit card bills prior to disposing of them. This includes pre-approved credit offers as well.

-Report lost or stolen checks immediately by calling 618-244-3000 so we can stop payment on the checks. Don't leave new check orders in your mailbox for extended periods of time and verify new deliveries have not been tampered with.

-Notify us promptly if your Visa debit card has been lost or stolen. Contact the main office at 618-244-3000.

-Protect your new, current and canceled checks. Always store checks in a safe place. When canceled checks have reached maximum retention, shred them prior to disposing of them.

-Review bills carefully. If they include suspicious items, investigate them immediately to head off any possible fraud before it occurs. Also, as much as you hate to receive bills in the mail, be sure they are arriving on time. If not, contact the company to find out why. Someone may have put a false change of address notice on you to divert your personal information to another address for his or her access.

-Never leave your checkbook, wallet or other personal information unprotected—even when you are at home. Workmen, contract laborers you may engage, or others that enter your house should not be able to gain access to your personal or financial information.

-Reconcile your banking statement immediately to assure your account activity is correct. Contact your local Community First Bank if any unauthorized transactions have occurred. Consider signing up for online banking as you will be able to monitor activity on your accounts 24x7 anywhere an internet connection is available.

-Review your credit report from the three major agencies at least annually to confirm there were no unauthorized credit inquiries made or accounts opened in your name. As part of the Federal Fair Credit Reporting Act, you are entitled to an annual free credit report from each of the three nationwide consumer reporting agencies through [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228. You can obtain a copy of your credit report at any time for a small fee through these three major credit bureaus:

### Major Credit Reporting Agencies

Equifax	1-800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	1-800-680-7289	<a href="http://www.tuc.com">www.tuc.com</a>

### Actions to Take if Your Identity Is Stolen

1. Immediately contact your bank and credit card providers by calling the phone number listed on your statements.

2. Contact the Federal Trade Commission (FTC) by one of the following methods:

**Internet** – [www.consumer.gov](http://www.consumer.gov)

**Phone** – 1-877-ID-THEFT (438-4338)

**Mail** – Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, D.C. 20580

The FTC is the clearinghouse for identity theft complaints and provides an ID Theft Affidavit which you should complete as soon as possible after you become aware of the fraud. Completing this affidavit can help protect you from responsibility for fraudulent charges on your accounts.

3. Contact the fraud division of the three major credit reporting agencies and request that a "fraud alert" be placed in your file. Ask that no new credit be granted without your approval. Request a copy of your credit report.

### Fraud Division of Major Credit Reporting Agencies

<b>Equifax</b>	1-800-525-6285
<b>Experian</b>	1-888-397-3742
<b>TransUnion</b>	1-800-680-7289

4. Cancel all accounts that have fraudulent activity or are at risk.

5. Contact your local law enforcement agency.

6. If your mail has been stolen, contact the U.S. Postal Service.

7. Keep detailed records of all events once you ascertain that your identity has been stolen. Include names, telephone numbers, and the date and time you made contact with individuals or companies requesting assistance in recovering your good name.