

### **What is Identity Theft?**

Identity theft is the fraudulent use of a person's personal identifying information. Identity Theft crimes are growing in substantial numbers. Linn Area Credit Union recognizes this trend and desires to inform and protect our membership from such a crime. To do this, we have compiled a resource kit that provides suggestions and strategies to aid in the prevention of Identity Theft, as well as, how to respond if you become a victim of Identity Theft.

### **What information does a person need to steal my identity?**

Any or all of the below information assists another person to steal your identity:

- Name
- Social security number
- Address
- Mother's maiden name
- Place of employment
- Telephone number
- And other related information about yourself

### **Why does Identity Theft happen?**

Identity thieves use another person's personal information, such as social security number, mother's maiden name, date of birth, or account number to open fraudulent new credit card accounts, write share drafts, charge existing credit card accounts, open share accounts, or obtain new loans.

### **How does Identity Theft happen?**

They obtain information by...

- Stealing wallets / purses that contain personal identification information and credit cards.
- Stealing your mail, including your financial statements, credit card statements, pre-approved credit offers, telephone calling cards, and tax information.
- Completing a change of address form to divert your mail to another location.
- Rummaging through trash for personal data.
- Stealing personal identification information from workplace records.
- Intercepting or otherwise obtaining information transmitted electronically.
- Shoulder surfing. Namely, overhearing your personal information when you are talking to someone in person or over the telephone.
- Fraudulently obtaining your credit report by posing as a landlord, employer, or someone else who may have a legitimate need for – and legal right to – the information.

### **The most common types of Identity Theft are...**

- Using or opening a credit card account fraudulently.
- Opening telecommunications or utility accounts fraudulently.
- Passing and / or cashing bad checks, withdrawing funds from another person's account, or opening a new credit union account under someone else's name.
- Getting loans in another person's name.
- Working in another person's name.

## How Can I Prevent Identity Theft?

While you can't prevent identity theft entirely, you can minimize your risk. By managing your personal information wisely, cautiously, and with an awareness of the issue, you can help guard against identity theft.

### Suggestions to Prevent Identity Theft:

1. *Do not give out personal information* such as account numbers or social security numbers over the telephone, through the mail, or over the internet, unless you initiated the contact and know with whom you are dealing.
2. *Store personal information in safe place* and shred old credit card receipts, ATM receipts, old account statements, and unused credit card offers before recycling them.
3. *Do not have your social security number, telephone number, or driver's license number printed on your checks.*
4. *Protect your PINs and other passwords.* Avoid using easily available information such as your mother's maiden name, birth date, last four digits of your social security number, and phone number, etc. Do not write down your PINs, memorize them!
5. *Order copies of your credit report* from each of the three major credit bureaus at least once a year to ensure that they are accurate.
  - Equifax # 1-800-525-6285
  - Experian # 1-888-397-3742
  - TransUnion # 1-800-680-7289
6. *Carry only the minimum amount of identifying information* and the number of credit cards that you need. Do not carry your social security card with you unless absolutely necessary.
7. *Keep a list of all your credit accounts and Linn Area Credit Union accounts in a secure place*, such as a safety deposit box. For your convenience, we have provided an Identity Theft Recovery Sheet and a Financial Institution Record to organize this information. Also keep tax records, cancelled checks, and paid bills in a secure place or shred before recycling them.
8. *Pay attention to billing cycles and statements.* Inquire with your utility companies if you do not receive a monthly bill / statement. It may mean that the bill / statement have been diverted by an identity thief.
9. *List only your name and number, without your address, in the telephone book.*
10. *Check Linn Area Credit Union account statements carefully* to ensure all charges, share drafts, and withdrawals were authorized. You may desire to place a code word on your accounts at Linn Area and with your credit card companies.
11. *Never leave your purse or wallet in your vehicle*, even if it's hidden.
12. *Guard your mail from theft.* If you have the type of mailbox with a flag to signal that the box contains mail, do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at a local post office. Promptly remove incoming mail. Request a vacation hold from the Postal Service when you are away from home.
13. *Remove your name from pre-approved credit offers, direct mail lists, and telephone solicitations.*
  - For pre-approved credit offers, call #1-888-5 OPT OUT (#1-888-567-8688)
  - For direct mail lists, write:  
DMA Mail Preference Service  
P.O. Box 9008  
Farmingdale, NY 11735-9008
  - For telephone solicitations write:  
DMA Telephone Preference Service  
P.O. Box 9014  
Farmingdale, NY 11735-9014

### **How Do You Know? The Biggest Problem:**

You may not know your identity's been stolen until you notice that something's amiss: you may get bills for a credit card account you never opened, your credit report may include debts you never knew you had, a billing cycle may pass without you receiving a statement, or you may see charges on your bills that you didn't sign for, didn't authorize, and don't know anything about.

### **What to Do If Your Identity is Stolen:**

The main thing to know is that this is not personal. Remaining calm will help you move through the processes involved. When an imposter uses your name, your Social Security number, your credit card number, or some other piece of your personal information for their use, it's Identity Theft. In short, when someone appropriates your personal information without your knowledge - it's a crime, pure and simple.

The first thing is to keep a record of all correspondence you have and place it in a central location. It is recommended to have a special envelope that you can keep all your written notes and documents of every written, telephone, and person to person interaction. You will want to keep all the documentation of the below listed items in such an envelope.

1. File a report with local police or the police where the identity theft took place. Get the case number and a copy of the police report in case the Credit Union, credit card company or others need proof of the crime later. In your ID Theft Affidavit, please see the Victim's Law Enforcement Actions section.
  - Cedar Rapids Police Department: Investigation Division # 319-286-5400
  - Marion Police Department # 319- 377-1511
  - Linn County Sheriffs Department # 319-892-6100
2. Contact the fraud departments of each of the three major credit bureaus, listed below. Tell them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.  
At the same time, ask the credit bureaus for copies of your credit reports. Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. In a few months, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

#### **Order Credit Report**

Equifax 800-685-1111

Experian 888-EXPERIAN (397-3742)

TransUnion 800-916-8800

#### **Report Fraud Web site**

800-525-6285

888-EXPERIAN

800-680-7289

[www.equifax.com](http://www.equifax.com)

[www.experian.com](http://www.experian.com)

[www.tuc.com](http://www.tuc.com)

3. Contact the creditors for any accounts that have been tampered with or opened fraudulently. This information can be taken from your completed Identity Theft Recovery Sheet and Financial Introduction Record, provided in your Resources Kit. Ask to speak with someone in the security or fraud department, and follow up in writing. Your ID Theft Affidavit packet will provide you with the forms necessary to send to your creditors. For any accounts that have been fraudulently accessed or opened, close them. Put passwords on any new accounts you open.
4. Call the ID Theft Clearinghouse toll-free at 1.877.ID.THEFT (1-877-438-4338) to report the theft. Counselors will take your complaint and advise you on how to deal with the credit-related problems that could result from ID Theft. The Identity Theft Hotline and the Identity Theft Website ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) give consumers one place to report the theft to the federal government and receive helpful information.

### **How to Manage the Most Common Forms of Identity Theft:**

Although identity thieves can wreak havoc on your personal finances, there are some things you can do to take control of the situation. Here's how to manage some of the most common forms of identity theft.

1. If an identity thief has stolen your mail for access to new credit cards, credit union and credit card statements, pre-approved credit offers and tax information or falsified change-of-address forms, he / she has committed a crime. Report it to your local postal inspector
2. If you discover that an identity thief has changed the billing address on an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. Avoid using easily available information like your mother's maiden name, your birth date, and the last four digits of your Social Security Number or your phone number. Avoid the same information and numbers when you create a Personal Identification Number (PIN).
3. If you have reason to believe that an identity thief has accessed your Linn Area Credit Union accounts or ATM / Debit Card, close the accounts immediately. When you open new accounts, insist on password-only access. If your checks have been stolen or misused, place a stop payment on these items. If your ATM / Debit Card has been lost, stolen or otherwise compromised, cancel the card and get another with a new PIN.
4. If an identity thief has established new phone or wireless service in your name and is making unauthorized calls that appear to come from - and are billed to - your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and calling card. Get new accounts and new PINs.
5. If it appears that someone is using your Social Security Number, get in touch with the Social Security Administration (SSA) to verify the accuracy of your reported earnings and that your name is reported correctly. Call (800) 772-1213 to check your Social Security statement.
6. If you suspect that your name or Social Security Number is being used by an identity thief to get a driver's license, report it to your Department of Motor Vehicles. Also, substitute another number on your driver's license than your Social Security Number. Iowa Department of Transportation # 319-377-6461.

### **Stay Alert**

Taking the steps outlined in this resource kit will guide you in resolving your identity theft problems. Keep in mind, though, identity theft or related credit problems may reoccur. Stay alert to new instances of identity theft. Notify the proper agencies and authorities, as listed in this resource kit.

### **Attachments:**

*ID Theft Affidavit Packet*  
*Identity Theft Recovery Sheet*  
*Financial Institution Record*