The United Federal Credit Union

Identity Theft

Protecting your identify is a serious matter. We at The United Federal Credit Union take identity protection seriously. It is important that you understand this risk. Below is a link to a document that discusses how your identity can be stolen and how you can prevent theft.

Identity Theft – Don't let it Happen to You

An identity thief works in a variety of ways:

• He impersonates you when he calls your credit card issuer and asks to change the mailing address on your credit card account. He runs up charges but you are unaware because bills are sent to another address.

• Using your name, date of birth, and Social Security number, she opens a new credit card account. Unpaid charges eventually show up on your credit report.

• He opens phone or wireless service in your name.

• A bank account is opened in your name and she writes bad checks on that account.

• To avoid paying debts he has incurred under your name, or to avoid eviction, he files for bankruptcy under your name.

• She counterfeits checks and debit cards and drains your bank account.

• He buys a car by taking out an auto loan in your name.

• She writes a letter to you, using letterhead stolen from a financial institution, stating that you must furnish your Social Security number to clear up a problem.

• He sends you a phony IRS form that requires personal information.

• With a stolen ID, she opens a bank account, takes out a loan using your address, then you are dunned for the payments never made on the loan.

You know you've had your identity stolen when:

• Your credit card bills show unauthorized charges.

• Your credit rating takes a major dip because of delinquencies on loans or credit cards of which you had no knowledge.

• You are denied employment, credit, loans, mortgages, government benefits, utilities and leases because your credit report and background checks show fraudulently incurred debts or wrongful criminal records. How a thief gets your personal information:

- By stealing your wallet or purse containing your identification, credit cards, and bank cards.
- By stealing your mail.
- By completing a "change of address" form to divert mail to another address.
- By rummaging through your trash at home or work for personal information.
- By posing as a landlord or employer in order to get personal information.
- By getting your business or personnel records at work.

The United Federal Credit Union

- By finding personal information in your home.
- By purchasing personal information from "inside" sources, such as paying a store employee for information you provided on a credit application.
- By using a pocket-sized scanner to get your credit card number when you present it for payment for goods or services.
- By fitting a false ATM front on a machine that "swallows" your ATM card.

Prevent ID Theft

1. All that a thief needs is your name, address, and Social Security number to do damage. If you don't already have one, get a paper shredder. Small, inexpensive ones are available. And use it for any mail you dispose of that contains sensitive information.

2. Once a year, order your credit report from all three credit reporting agencies (See Important numbers below). Make certain there are no inaccuracies.

3. Read your account and credit card statements as soon as they arrive. Look for unauthorized transactions. If your bills don't arrive on time, follow up with creditors. A missing credit card bill could mean an ID thief has control of your credit card account and changed your billing address.

4. Keep your Social Security number off your checks and driver's license and out of your wallet or purse. Unless absolutely necessary, do not divulge your Social Security number to anyone.

5. Only carry your extra credit cards, birth certificate, or passport with you when you need to. Use as few credit cards as you can.

6. Secure personal information in your home, especially if you have roommates or employ outside help of service workers.

7. When you need new checks, order them with your first initial and last name only.

8. Photocopy both sides of your driver's license, ATM, credit, debit, and health insurance cards, and any other items you carry, and put the copies in a safe place. You'll have the phone numbers you'll need in case your wallet or purse is stolen. 9. Don't provide, or confirm, personal information to a telephone solicitor unless you initiated the call. Before releasing personal data, learn how it is to be used or if it will be shared with others.

10. Retrieve your mail from your box as soon as you can. Keep a lock on it. Put outgoing mail in post office collection boxes. If you're going away for a period of time, call your local post office and request a hold.

11. See about having passwords or extra security protection put on your credit card, credit union, and telephone company accounts.

12. Choose passwords and PINs that are not predictable. Avoid using the last four digits of your Social Security number, your middle name, or birth date.

13. Don't keep passwords or PINs in your purse or wallet.

14. Shield your PIN from curious onlookers when using an ATM.

15. Once a year, order your Social Security Earnings and Benefits Statement from the Social Security Administration to verify that your information is accurate.

16. If you plan to provide personal information online, make sure the site displays a locked padlock symbol in the lower right corner of your browser, ensuring it has an encrypted connection. Don't deal with sites that ask for more than your name, address, phone number, and credit card number.

17. Regularly update your virus protection software.

18. Don't download fi les sent by strangers or click on hyperlinks from e-mail senders you don't know.

19. Install a fi re wall program, especially important for a high-speed Internet connection, to prevent hackers from getting to your computer.

20. Be careful about storing financial information on your laptop computer. Often they are stolen for the information they contain.

21. Before you throw out any compact disks, check for any that may contain personal information such as Social Security number or PINs and destroy them.

22. Each of the three major credit reporting agencies has its own credit monitoring service—available for a fee—which sends you e-mail alerts of any credit activity posted to your file.

If You are a Victim

Notify your financial institution to contact you if there is any unusual activity on your account.

Change your PINs. Contact police in the jurisdiction where the theft took place. File a report and keep a copy for yourself. Call your postmaster if you think the mail was used.

Call the fraud divisions of one of the credit reporting agencies and request that a "fraud alert" be placed on your name and Social Security number. Reporting fraud to an agency will require any company or creditor to contact you to authorize any new credit. Ask for copies of your reports. As a victim of identity theft, you'll get them free. Follow up your call with a letter and enclose a copy of the police report. By doing this, you are protected legally should the agencies fail to remove the crime from your record.

Call the creditors who opened accounts in your name. Inform them of the identity theft and close the accounts. Get copies of all transactions and applications on the accounts.

Contact the Federal Trade Commission at 877-IDTheft. Request and file the ID Theft Affidavit that alerts companies and organizations that may have fraudulent accounts opened in your name.

To report identity theft, contact one of these credit reporting agencies:

TransUnion 800-916-8800

www.transunion.com

The United Federal Credit Union

Experian 888-397-3742

www.experian.com

Equifax 800-685-1111

www.equifax.com

Important Numbers

Federal Trade Commission Identity Theft

Hotline: 877-IDTheft (877-438-4338)

For online ID theft:

www.consumer.gov/idtheft/

To receive your free credit report by phone, mail or online:

annualcreditreport.com or call 877-322-8228

Social Security statement request:

800-772-1213 or www.ssa.gov/

Identity Theft Resource Center (non-profit):

858-693-7935 or www.idtheftcenter.org

To report ID theft it is only necessary to call one credit reporting agency. Within 24 hours, each bureau will attach a fraud alert to your credit fi le. The single call also opts you out of all preapproved offers of credit or insurance for two years, and will get you a mailed copy of your credit file.