

### **Identity theft can happen to anybody.**

Identity theft is on the rise - 7-10 million individuals will fall victim to this crime each year. 27.3 million Americans have been victims of identity theft in the past five years, and the crime has increased noticeably in the past year, which accounted for 9.91 million of those victims. Half of these victims did not know how their information was obtained or misused. With nearly 5% of the population affected by identity theft in the past year alone, an 80% increase from the previous year, it is important to understand how to protect yourself by taking certain precautions.

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

There are two types of identity theft – account takeover and application fraud. “Account takeover” occurs when a thief takes your credit account information and then purchases products and services by either using the actual credit card or just the account number and expiration date. “Application fraud” (also known as “true name fraud”) is when a thief uses your Social Security Number and other identifying information to open new accounts in your name. It is difficult for a person to discover that they are a victim of “application fraud” because the monthly account statements can be mailed to different addresses used by the thief, whereas victims of “account takeover” find out when their monthly account statements come in the mail. Victims of identity theft are often left with a bad credit report and spend many months and years trying to get their financial information under control. Victims also have difficulty getting credit, obtaining loans, renting apartments, and getting hired.

### **How is This Personal Information Misused?**

- ✓ 26%, or 2.5 million people, reported that they did not realize suspicious account activity by companies such as credit card issuers and banks.
- ✓ 8% of individuals reported that they found out they were victims of identity theft when they applied for credit and were turned down.
- ✓ 15% of all victims reported that their personal information was misused in non-financial ways, such as to obtain government documents or on tax forms.
- ✓ 67% of victims reported that their existing credit cards were misused.
- ✓ 19% reported that their checking or savings accounts were misused.
- ✓ 25% of all victims reported that their information was lost or stolen via credit cards, checkbooks, or Social Security cards.
- ✓ 400,000 people last year fell victim to this crime

asa result of stolen mail.

### **How Thieves Get Your Personal Information**

- ✓ "Dumpster diving" in garbage bins and roadside storage containers for unshredded credit card and loan applications and documents containing personal information, such as Social Security/ account numbers.
- ✓ Stealing mail from mailboxes to take bank and credit card statements, newly issued credit cards, pre-approved credit cards, investment reports, insurance statements, and tax information.
- ✓ Posing as an employer, loan officer, landlord, etc. in order to access a person's credit report illegally.
- ✓ Obtaining sensitive information, such as names, account and Social Security numbers, and passwords from personnel or customer files in the workplace.
- ✓ "Shoulder surfing" (looking over another person's shoulder) at ATM machines in order to look at PIN numbers.
- ✓ Finding identifying personal information on internet sources through public records and fee-based information broker sites.

### **How Much Does Identity Theft Cost?**

- ✓ 40% of identity theft victims paid real "out of pocket" expenses (as well as time and energy spent fighting the expenses and damages incurred); these 14 million Americans ended up paying \$3.8 billion in the past two years.
- ✓ Victims' losses average \$740 each.

### **How to Reduce Your Chances of Becoming A Victim of Identity Theft**

#### **Reduce Access to Your Personal Information**

- ✓ Never carry extra credit cards with you that you do not use. Never carry your Social Security card, birth certificate, or passport. Carry these items only when you need them.
- ✓ Always hold onto your wallet and purse or keep them locked away.
- ✓ Be sure that other items or cards in your wallet or purse do not contain your Social Security number and only give this number out when absolutely necessary. Be sure to ask if it is necessary to give your Social Security number in various situations, such as when making certain purchases, as you will find out that it is not always necessary to give out this number.
- ✓ Reduce the amount of unnecessary personal

information that is public, such as by removing your name from the marketing lists of the three credit reporting bureaus -- Equifax, Experian and Trans Union. You can do this by calling **888-5OPTOUT**, which will limit the number of pre-approved offers of credit that you receive. By receiving fewer of these offers, you limit the valuable personal information left in your mailbox.

- ✓ Sign up for the Federal Trade Commission's "National Do Not Call" Registry and the Direct Marketing Association's Telephone Preference Service. Your name is then added to deletion lists, limiting the amount of mail sent to your house with personal information. The number for the National Do Not Call Registry is (888) 382-1222, or you can go to [www.donotcall.gov](http://www.donotcall.gov).
- ✓ Choose not to sell or share your financial information when asked by your bank, credit card companies, insurance companies, and investment firms. Never give out more information than you have to, and always ask whether it is necessary for you to give out certain personal information, such as your Social Security number or other family members' names.
- ✓ Install a locked mailbox at your residence to deter mail theft, and always pick up your mail as soon as possible. When you go on vacation or are gone for an extended period of time, have your mail held at the post office or ask a family member or close friend to pick it up for you.
- ✓ Pick up your checks at the bank, and pick up other confidential information that you would have sent to your house whenever possible.
- ✓ When paying bills, mail them at drop boxes inside the post office rather than leaving them in your mailbox, as your checks can be stolen and altered. Do this whenever sending personal and confidential information.

#### **Credit Cards and Credit Reports**

- ✓ Reduce the number of credit cards you actively use, and only carry the one or two cards that you regularly use in your purse or wallet. You may also want to cancel unused accounts.
- ✓ Always keep a list or photocopies of all credit cards, bank accounts, and investments in a secure place (such as a safe or safety deposit box), so you can quickly contact these companies if you lose a card or think you may be a victim of identity theft.
- ✓ Never give out your Social Security number or other personal information over the phone (or by

mail or on the Internet) unless you have a trusted business relationship with the company and you started the call. Many people can call with bogus stories, such as winning a trip, in order to get this information.

- ✓ When shopping, always keep your credit card receipts in your wallet or purse, not in the merchandise bag.
- ✓ Never allow your credit card number or Social Security number to be written on checks or random sheets of paper.
- ✓ Order a credit report two times a year in order to check for errors and fraudulent use of your accounts. Closely watch other accounts for suspicious activity.
- ✓ Place a "fraud alert" on your credit reports. These alerts place a statement in your file requesting credit issuers to call you at your phone number before issuing credit. If an imposter is trying to open credit in your name, you should get a call from the credit grantor first.

#### Passwords and PIN Numbers

- ✓ When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, your mother maiden name, your birth date, pet's name, consecutive numbers or anything else that other people could easily know about you. It best to create passwords that combine letters and numbers, and never write your passwords down in order to remember them. Try to memorize them or keep them written down on paper that is locked in a secure place.
- ✓ Shield the screen when using an ATM machine or making long distance phone calls with your phone card. Always be aware of who may be watching you.

#### Protecting Information Handling

- ✓ Install a firewall on your home computer to prevent hackers from obtaining personal information and financial data from your hard drive. Password-protect files that contain sensitive personal data and account information.
- ✓ Request that financial institutions adequately safeguard your data and inquire about how they do this. When filling out applications or

forms that request personal information, find out how the company disposes of these forms when they are done with them. Also, find out how businesses store and dispose of information when you use your credit card.

- ✓ Always store personal information securely in your home and properly dispose of items that contain sensitive information, preferably by shredding these documents.

**More information on identity theft and other ways to safeguard personal privacy can be found at [www.privacyrights.com](http://www.privacyrights.com); the Federal Trade Commission (<http://www.consumer.gov/idtheft/>); and the Minnesota Attorney General's website <http://www.ag.state.mn.us/consumer/privacy/GuardingYPrivacy>**

---

To make an appointment, please call our office at 612/624-1001. The receptionist can explain our eligibility requirements, answer questions about the scope of our practice areas, and refer you to other services or agencies that might be able to help. Please note that USLS cannot take cases where the adverse party is the U of M or any of its departments, staff, or students. Please see the *USLS Handbook* for the full text of all USLS client policies.: [www.umn.edu/usls](http://www.umn.edu/usls).

**PLEASE NOTE: The materials contained in this pamphlet have been prepared for information and educational purposes only. Communication of information through this pamphlet does not create or constitute an attorney-client relationship, is not intended to solicit clients or to provide legal services as to any particular matter and is not intended to convey or constitute legal advice or provide a substitute for obtaining legal advice from a qualified attorney. It is important for you to consult with an attorney regarding your rights and responsibilities in a particular situation.**

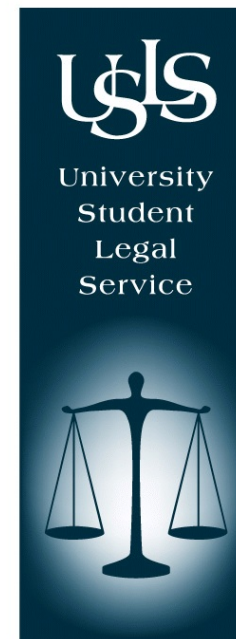
The University of Minnesota is an equal opportunity educator and employer.

© 2004 by the Regents of the University of Minnesota. All Rights Reserved.

This publication is available in alternative formats. Please contact USLS at 612/624-1001. *Revised 3/2009*

# What Students Need to Know About Identity Theft

UNIVERSITY OF MINNESOTA



## University Student Legal Service

160 West Bank Skyway  
219 19<sup>th</sup> Avenue South  
Minneapolis, MN 55455  
Phone: (612) 624-1001  
Fax: (612) 624-7351  
[www.umn.edu/usls](http://www.umn.edu/usls)