



Identity Theft on Campus

From the Office of Minnesota Attorney General Mike Hatch

Everybody knows that you have to protect your wallet to guard your cash from potential thieves. But across college campuses, students are at risk of having something even more important stolen: *their identity*. In the past, thieves sometimes scoured dorm rooms and student centers for cash. Today, however, they also look to steal personal information, such as your identification card, billing statements, social security number or other documents containing your private information. Other identity thieves may try to convince you to disclose your information over the telephone or internet, by impersonating a company that you do business with, or your college. Don't fall for these tricks!

Once identity thieves steal your information, they can assume your identity and run up thousands of dollars in unauthorized credit *in your name*. Identity thieves can also use your banking information, such as the check routing numbers at the bottom of your checks, to withdraw money from your account. Don't let this happen to you!

I. Don't Be an Easy Target

Secure Your Information on Campus. Make sure your dorm room or apartment is secure. These locations can be easy targets for identity thieves if security is lax. Guard your credit and debit card numbers. Identity thieves staring over your shoulder can obtain your account numbers and use them to access your credit. Similarly, if you leave your card somewhere, such as on a restaurant table, the information may be susceptible to theft. In such cases you may wish to cancel the card, or obtain a new account number. Do *not*, in any case, lend your card out to other individuals.

Protect Your Credit Cards, Checks, and Billing Statements. Credit cards, checks, and billing statements contain all the information necessary to steal an identity. Students should remove extraneous

information such as their middle name, phone number, Social Security number or driver's license number when ordering new checks. Students should not use any combination of numbers that could be easily detected by thieves when creating passwords and personal identification numbers ("PINS"). Students should not use the last four digits of their Social Security number, birth date, middle name, mother's maiden name, address, or consecutive numbers as identification or PIN numbers.

Be Smart with Credit Cards. Students should not give out their credit card number or other personal information over the phone or internet unless they know with whom they're doing business. Even then, before revealing any personal information, students should find out how it will be used or shared with others. Also, check for fraudulent use of credit accounts. Once a year, consumers may order a copy of their credit report from the three largest credit bureaus. Under Minnesota law, consumers can obtain a credit report for \$3 per credit bureau once every year. Contact the Attorney General's Office to request *Credit Contact Information*, a free one-page flyer that contains an order form to use when requesting a credit report, or obtain it online at www.ag.state.mn.us.

Be Smart Online. The Internet puts vast information at everyone's fingertips. Before shopping, though, students should make sure that they are familiar with the company or seller, including its privacy policy. Disclose only necessary personal information and opt-out of possible information sharing.

Beware of Phone and Email Scams. Be on guard against phone calls and emails impersonating financial institutions or other businesses that ask a consumer to disclose their banking information. Perpetrators of this scam copy the logos of businesses and send mass emails, which claim that the company experienced security or

computer problems and needs to update a customer's information or risk having their account frozen. The emails ask unsuspecting consumers to click on a link, which then directs them to an internet site which appears to be managed by the business in question. In reality, the scam artists have manipulated the URL (the web page address) to mimic that of the legitimate business. Do *not* respond to such fraudulent requests to disclose information. If students have questions about the validity of such a request, call the business in question and talk to them first.

Tear up Financial Information. Don't toss credit card convenience checks or pre approved credit offers in the trash or recycling bin before first tearing them into small pieces or shredding them. The solicitations can be used by "dumpster divers" to cash the checks or order credit cards in a consumer's name. In addition, students should destroy other sensitive information like credit receipts, bank statements, and important bills they do not retain for their records.

Monitor Your Records. Carefully review records, including credit card statements and mortgage statements, for unauthorized charges or fraudulent use. In addition, students should scrutinize local, long distance, and cellular phone bills each month and report any unauthorized use to their service provider and local law enforcement agencies.

II. What Students Should do if Their Information is Stolen

1) Contact Your Local Law Enforcement Agencies. Contact the police immediately to fill out a police report. Police frequently work with banks and other agencies to apprehend identity thieves.

2) Contact Banks and Credit Card Companies. Immediately alert financial institutions of the fraud and stop potential unauthorized transactions on the consumer's account. Close accounts that have been jeopardized by identity theft. Change all account numbers and passwords.

3) Contact the FTC to File a Fraud Affidavit. The FTC maintains an Identity Theft Clearinghouse and works in conjunction with other law enforcement agencies to combat Identity Theft. Contact the FTC as follows:

Federal Trade Commission
Identity Theft Clearinghouse
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
TDD: (202) 326-2502
www.consumer.gov/idtheft

4) Contact the Social Security Administration. Students should call the Social Security Fraud Hotline at 1-800-269-0271 if they believe someone may be misusing their Social Security number.

5) Contact Credit Reporting Agencies to Place a Fraud Alert on All Credit Reports. Immediately contact the three major credit bureaus as follows:

Equifax: 1-888-525-6285
Transunion: 1-800-680-7289
Experian: 1-888-397-3742

6) Contact the Minnesota Attorney General's Office. The Attorney General's Office publishes a free brochure, *Guarding Your Privacy*, which contains more information on identity theft. This, and other information, is also available at the Office's website in the *Privacy* section. To obtain more information on identity theft, contact:

Office of Minnesota Attorney General Mike Hatch
1400 NCL Tower
445 Minnesota Street
St. Paul, MN 55101
(651) 296-3353
1-800-657-3787
TTY: (651) 297-7206
TTY: 1-800-366-4812
www.ag.state.mn.us/consumer