

# The Keys to **PROTECTING YOUR IDENTITY**

A RESOURCE FOR EMPLOYEES OF ALLINA HOSPITALS & CLINICS



**ALLINA**<sup>®</sup>  
*Hospitals & Clinics*

# Welcome to Your Identity Theft Toolkit

## Dear Fellow Employees:

If you've been following the news, you've likely noticed that identity theft is a growing problem — and it seems to be picking up speed. In fact, identity theft is the fastest growing financial crime in the United States.

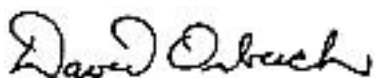
We live in what's been called "the information age." Through use of the internet, e-mail, fax machines, and cellular phones, we have access to more people and information than ever before. While these technological advances have made communications easier and faster, they've also opened up a host of new risks, particularly for financial institutions and health care organizations.

Several employees have recently asked what Allina is doing to combat the threat posed by identity thieves. Allina is committed to protecting patients and employees from the misuse of their personal information. This commitment is embodied in Allina's mission and values, through which we pledge to act in the best interests of our patients — and one another.

I'm please to present to you this identity theft "toolkit" to help you understand the nature and impact of identity theft and provide you with information and resources you need to reduce your risks, as well as protect our patients and the communities we serve.

Thank you for your attention to this important issue. If you have any questions or comments about identity theft, please contact me at 612-775-5819 or [david.orbuch@allina.com](mailto:david.orbuch@allina.com). I welcome your comments and feedback as we continue to address the issue of identity theft within Allina.

Sincerely,










David Orbuch  
Executive Vice President, Compliance & Public Policy  
Allina Hospitals & Clinics

## WHAT IS IDENTITY THEFT?

Identity theft occurs when a person "steals" your name, social security number, or other personal information and then misuses that information to open new accounts, charge expenses or conduct other fraudulent activities in your name. By stealing your name and personal information, identity thieves hope to leave you stuck with the bill and, possibly, credit problems that can take a significant amount of time and money to repair.

### Identity thieves use a number of methods to obtain your personal information, including:

-  Stealing wallets and purses
-  Stealing mail or submitting a change of address form in order to divert your mail to another address
-  Digging in trash receptacles, drawers and personal belongings
-  Using computer and telephone scams to induce consumers to provide personal information
-  Accessing personal information through computer systems to which the thief has access
-  Posing as a loan officer and ordering a copy of your credit report (which lists account information)
-  "Shoulder surfing" at ATMs to obtain personal identification numbers (PINs) and account information.

## Case studies

### 1. "Phishing" for your identity

You receive an e-mail from a company with whom you do business informing you that there is a problem with



their account.

The e-mail directs you to a company Website. When you get to the Website, you're asked to provide your social security number and other personal information so that the problem

can be "fixed." In actuality, the e-mail came from identity thieves who set up a fake Website and e-mail address to obtain your personal information.

Experts advise that if you receive an e-mail that appears to come from a reputable company, avoid filling out any forms attached to the e-mail message. Instead, enter the company's official Web address and visit the site to determine if the company is truly experiencing problems.

### 2. One person's trash becomes another person's treasure

You work in a health care facility which has a locked recycling container for the disposal of confidential patient information, including insurance information, social security numbers, and addresses. When taking some documents to the recycling area, you notice that someone has placed a stack of documents containing patient information in a nearby trash can.

In this situation, you should immediately remove the confidential information from the trash can, place it in the locked recycling container, and contact your supervisor.



## IT'S MORE COMMON THAN YOU THINK

According to law enforcement officials, identity theft is the fastest growing financial crime in the country, with more than 161,000 reported victims in 2002 with 1,873 cases reported in Minnesota and 1,777 cases in Wisconsin.

## Allina's experience with identity theft

Allina, like many other health care organizations, has experienced identity theft first-hand. An identity theft incident occurred on the Abbott Northwestern campus in 2002 when an employee of Sister Kenny Institute stole social security numbers from patient information cards. The employee then gave the information to others who opened fraudulent credit card and telephone accounts in the patients' names. The former employee recently pleaded guilty and will provide assistance in the prosecution of others involved in the theft.

Allina is also investigating whether a former employee of another Allina Hospital stole stickers used on patient medical records. The stickers contain the patient's name, social security number and birth date. The former employee may have used this information to open credit cards in patients' names and fraudulently used the cards to purchase goods.

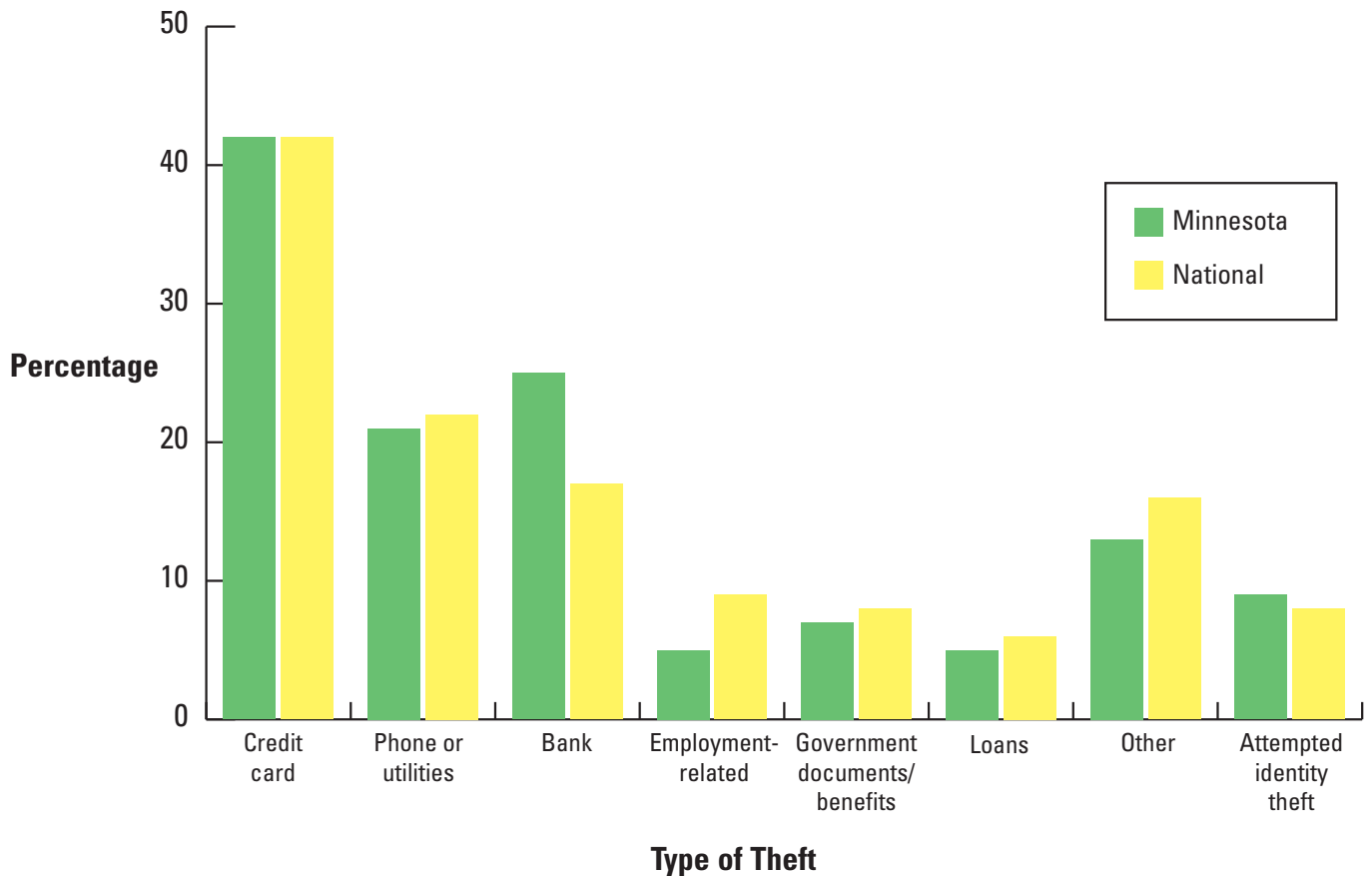
Allina is currently working with representatives of information services, security, legal, risk management, human resources, media relations and compliance to develop investigation protocols to ensure that we are able to promptly and effectively respond to incidents of identity theft.



## 3. Are you sure your leg isn't broken?

While out grocery shopping, you accidentally lose your wallet. The wallet contained all of your credit cards, checks, driver's license and insurance information. After reporting the missing credit cards, asking your bank to stop any stolen checks, and obtaining a new driver's license, you assume you've covered all of your bases. Six months later, you receive a bill from your health insurance company for thousands of dollars in services, including a trip to the emergency department. Yet, you never visited the emergency department. You realize that when your wallet was stolen, you forgot to contact your health insurance provider. Now, you have to make numerous calls to the hospital and insurance company to prove that someone made fraudulent use of your health insurance information. When you lose documents, cards or personal items that include your social security number, insurance policy numbers, credit cards, and other personal information, make sure you immediately inform every business with which you have an account or policy.

## Percentage of Victims by Type of Identity Theft



Source: Federal Trade Commission

The number of victims has risen considerably in the last year. The Federal Trade Commission ("FTC") recently conducted a comprehensive study of identity theft in the United States. The FTC found that an estimated 9.9 million people were victims of identity theft in the past year.

### IDENTITY THEFT IS EXPENSIVE AND TIME CONSUMING

According to the FTC, identity theft costs Americans \$5 billion per year. Moreover, identity theft costs businesses and financial institutions \$48 billion in lost revenues. When identity thieves rack up charges in another person's name, it's often the credit card companies, banks, and retailers who are left holding the bill. Ultimately, these costs are passed on to the consumer.

In the FTC's survey, victims of identity theft stated that, on average, they spent 30 hours resolving problems associated with the theft. Some victims spend months — even years — cleaning up the mess left by identity thieves.










Chris was so fed up with receiving numerous pre-approved credit card offers through the mail every day that he started throwing them away without even opening them. Chris's lease was up at his apartment and he was excited about the prospect of moving into a new place—and hoping that the credit card companies wouldn't bother him at his new address. However, after he submitted a credit application to the building's landlord, he was turned down for having "bad credit." Chris was stunned; he always pays his bills on time and carries a low balance on one of his credit cards. He called one of the credit reporting agencies and learned that two credit card accounts had been opened in his name and someone had charged more than \$10,000 in merchandise to those accounts. Someone accepted one of those pre-approved offers Chris threw away and Chris spent more than six months living with friends, taking time off of work, and spending countless hours on the phone in order to clear his name.

## PREVENTING IDENTITY THEFT






There are numerous, relatively simple steps you can take to prevent identity theft.

### Preventing patient identity theft














-  If your job involves caring for patients or handling patient data, do not leave identification bracelets, charts, or other documents containing social security numbers or other personal information in public view.
-  Medical charts must be stored in secure locations, preferably in locked drawers to prevent public access to the information.
-  Shred or store patient data in accordance with safeguard policies.
-  If you have patient information or data on your computer at work, utilize a screensaver or turn off your monitor if you step away from your desk.
-  Minimize your discussions about patients within hearing distance of visitors, other patients, and providers who are not involved in their care. When such discussions are necessary, exclude patient-identifying information (such as the patient's name or address) to the extent practical.
-  Take appropriate steps to ensure that when transmitting confidential information via fax, mail or e-mail, the information gets the intended recipient. Contact the recipient and alert them that the information is coming, and follow up with them to ensure that the information was actually received.
-  When sending confidential patient information via e-mail to others outside of Allina, use Allina's e-mail encryption software to ensure that the information is protected. For more information about encryption, contact Allina's Technology Services Center at 612-775-1900.

For more information about safeguarding confidential patient information, see Allina Privacy Compliance Policies at [http://akn/corp\\_compliance/privacy\\_policies.html](http://akn/corp_compliance/privacy_policies.html).

### Preventing theft of your own identity

-  Keep your wallet in a safe place at work, such as in a locked drawer or cabinet.
-  Don't carry your social security card or birth certificate in your wallet or purse.
-  Don't provide your social security number unless it is absolutely necessary. Ask why the other person needs it and whether you may provide a different identifier.
-  Carry only the credit cards that you need.
-  When ordering checks, don't put your driver's license number or social security number on them.

## Preventing theft of your own identity

-  Don't use the same personal identification number (PIN) for all accounts.
-  Avoid using PIN numbers and passwords that are easily detectable (your birth date, phone number, zip code, mother's maiden name). Use a combination of letters and numbers.
-  Keep all credit or debit card PIN numbers separate from the cards.
-  Change PIN and passwords frequently.
-  Don't give your credit card number over the phone unless you initiated the call or are certain that the transaction is legitimate and secure.
-  Shred any credit card receipts or statements containing account numbers and information before throwing them away.
-  Keep a list of all credit and debit accounts, account numbers and PINs. Place the list in a secure location.
-  Shred all pre-approved credit card offers.
-  Order a credit report from each of the three credit bureaus (Equifax, Experian, and TransUnion) annually to make sure the information is accurate.
-  Consider writing "See ID" on the back of your credit cards rather than signing them.
-  Don't place outgoing mail in your home mailbox. Place it in a secure, postal service collection box.
-  Pay attention to your billing cycles and, if you notice that a bill has not arrived on time, contact the company to determine whether a bill was sent and determine if your mail has been diverted by an identity thief.
-  Closely review your credit card statements for any unusual or unauthorized charges.

### CATCHING IDENTITY THEFT EARLY IS KEY

According to the FTC, the costs associated with identity theft—both in terms of time and money—go down significantly if the theft is discovered quickly. In general, those who discover that their identity had been stolen within six months spend substantially less time and money resolving the problem.

### ASK FOR HELP: REPORTING IDENTITY THEFT

The FTC survey revealed that only 25 percent of identity theft victims actually report the crime to law enforcement. Furthermore, only 22 percent of victims reported the theft to one or more of the credit bureaus. Reporting incidents of identity theft to both police and credit bureaus can assist greatly in stopping fraudulent activity in its tracks and help you prove to financial institutions and others that the activity occurred without authorization.

## Checklist

### IF YOU'RE A VICTIM OF IDENTITY THEFT: A Checklist to Follow

- File a report with local police. Credit card companies, banks, and other vendors may require a police report as proof that your identity was stolen. Retain several copies of the report and make note of your report number.
- If you discover that someone has opened an account (credit, phone service, etc.) in your name, immediately contact the company or bank that provided service or extended credit in your name and inform them of the theft. Follow-up your conversation with notice to the company in writing, accompanied by a copy of the police report. Document your conversations and keep a paper file of all correspondence. You may also be able to obtain a copy of the credit application, which may help you determine what information was stolen and may even lead to the identity of the thief.

Contact all three credit bureaus (Equifax, Experian and TransUnion) immediately. You must call all three because the individual bureaus do not necessarily share information. Order copies of your credit report from each bureau. Ask each of them to place a fraud alert on your account. Once a fraud alert is in place, the credit bureaus will not process credit applications without first obtaining your permission.

Equifax: 800-525-6285 or

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

Experian: 888-397-3742 or

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

TransUnion: 800-680-7289 or

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

The Consumer Credit Counseling Service may also be able to assist you in clearing fraudulent purchases and accounts from your credit report. Call 800-388-2227. You may also wish to consult a lawyer if you are having trouble removing fraudulent entries on your credit report.

- Change all personal identification numbers (PINs) and passwords. Choose unique PINs and passwords rather than common ones (i.e., your mother's maiden name, your birth date, etc.)
- Visit the FTC Website at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) and fill out the universal affidavit to submit to creditors.
- Contact the FTC directly for assistance. Call the toll-free hotline at 1-877-IDTHEFT or fill out a report online at [www.ftc.gov/ftc/complaint.htm](http://www.ftc.gov/ftc/complaint.htm).
- If your social security number was used inappropriately, contact the Social Security Administration's fraud hotline at 800-269-0721.
- If the thief uses your health insurance information without authorization, contact your insurer and inform them of the inappropriate use. Follow up with a letter documenting the situation and request that the insurer issue a new policy number.
- In the case of stolen or misdirected mail, contact the U.S. Postal Service at 800-275-8777 to obtain the number of your local U.S. Postal Inspector.
- For stolen passports, contact the U.S. Department of State at [www.state.gov](http://www.state.gov).
- If the thief has stolen checks, contact both check verification companies: Telecheck (800-366-2425) and the International Check Services Company (800-526-5380). They can place a fraud alert on your account to ensure that counterfeit checks will be refused.
- If the thief has used your driver's license number to write bad checks, contact Driver and Vehicle Services. You may need to obtain a new driver's license number and card.

## Exercise your Legal Rights

There are numerous federal and state laws in place to protect victims of identity theft.

### Federal laws

#### *Identity Theft and Assumption Deterrence Act*

Passed in 1998, the Act makes it a federal crime when an individual:

“knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.” See 18 U.S.C. § 1028(a)(7).

#### *The Health Insurance Portability and Accountability Act (HIPAA)*

The privacy and security provisions address the need to keep patient information confidential. The rules require that protected health information be used only for legitimate business purposes and that reasonable safeguards must be implemented to protect that information. Also, the privacy rule requires tracking of disclosures of protected health information.

#### *Fair Credit Reporting Act*

This act provides that credit organizations may only access your credit information for legitimate business reasons. Moreover, the law requires them to follow certain procedures in correcting errors on your credit report.

#### *Fair Credit Billing Act*

Establishes procedures credit card companies must follow in resolving billing errors. It also limits consumer liability for fraudulent credit card charges.

### State laws

#### *Minnesota*

Under Minnesota law, it is a crime for a person to transfer, possess, or use an identity that is not the person's own, with the intent to commit, aid, or abet any unlawful activity. Violation of the law may result in imprisonment and payment of court-ordered restitution to victims. See Minn. Stat. § 609.527.

#### *Wisconsin*

Similar to Minnesota law, Wisconsin makes it illegal for a person to use another's identity for unlawful purposes. Those found in violation of the Wisconsin law must serve jail time or pay fines of up to \$10,000. See Wis. Stat. § 943.201.

## Conclusion

Allina Hospitals & Clinics is committed to protecting patients and employees from identity theft. If you have questions or concerns, please consult one of the resources listed in Appendix D.

### Appendix B: Q & A

#### Your Questions

#### Our Answers

**Q: Health care organizations use social security numbers to identify patients and access patient information. Will Allina continue to use social security numbers this way?**

**A:** Eliminating the use of social security numbers in the health care industry is more problematic than many realize. The social security number is an important, unique identifier that is widely used by the government and others to identify and bill patients for health care services. Many health care providers and insurers have reduced the need to use social security numbers as patient identifiers by assigning unique patient identification numbers that are “tracked” to patients’ social security numbers. For example, a patient’s insurance card will state that the patient’s unique identifier, or member number, is 123456. When the patient’s identification number, 123456, is entered into the computer system, the screen will display both the patient’s unique identifier number and social security number. The social security number is then used to generate a bill.

Allina is also working to ensure the protection of patient and employee social security numbers. First, social security numbers will be removed as patient identification numbers on Medica insurance cards in 2004. However, like the example above, an individual’s social security numbers will still be one of the data elements in an individual’s account. Most other local insurers have developed similar systems to reduce the use of social security numbers on insurance cards.

Social security numbers are also used in clinical settings to identify and track patients. Some Allina hospitals utilize patient social security numbers; others do not. Through the implementation of an automated medical records system, however, we are working to develop a uniform system that will not require the use of social security numbers.

**Q: Will the use of automated medical records eliminate the risks of patient identity theft?**

**A:** While the implementation of an automated medical records system may not eliminate the risks of identity theft entirely, it will help reduce them in several ways. First, because all medical records will be computerized, business units will be able to reduce the “paper trail” and better control access to confidential patient information. Second, as mentioned above, patients will be assigned unique identifiers, which will reduce the need for providers to use sensitive social security numbers to track patient progress and generate patient bills. Finally, the automated medical records system will allow Allina to track and review access to patient records and to better detect inappropriate access to, and misuse of, sensitive information.

### **Q: How does the HIPAA Privacy Rule relate to identity theft?**

**A:** The HIPAA Privacy Rule requires health care providers to take reasonable steps to restrict work-force members' access to protected health information (information that identifies an individual or relates to their health care treatment) to the "minimum necessary" to accomplish the intended purpose of that access. Each business unit within Allina has adopted measures to ensure that protected health information is accessed only when needed to carry out legitimate work activities. Furthermore, each business unit must implement reasonable procedural and physical safeguards to protect the security of protected health information and track all authorized disclosures of that information.

Adherence to the requirements of the HIPAA Privacy Rule will further enable business units maintain patient privacy and prevent unauthorized access and distribution of sensitive patient information.

### **Q: What is identity fraud? Is it different from identity theft?**

**A:** Identity theft and identity fraud are two sides of the same coin. Identity theft involves taking personal information of another to conduct fraudulent activities in the victim's name. In essence, the thief "takes" the identity of the victim. With identity fraud, the perpetrator poses as another person to obtain services. For example, if a patient uses a counterfeit or stolen insurance card in order to obtain health care services, the patient has committed identity fraud.

### **Q: What should I do if an incident of identity theft occurs at work?**

**A:** A team of Allina employees is working to develop a protocol for reporting and investigating identity theft. Until the protocol is finalized, incidents of identity theft should be reported to security personnel at the business unit, or employees may contact the Allina Legal Department at 612-775-5862.

## Appendix C: Form letter

If you are a victim identity theft, the government has developed a form letter that consumers may use to communicate with banks and creditors. To view the letter, visit <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>

## Appendix D: Resources

### Helpful Websites

Minnesota Office of the Attorney General  
Consumer Protection Division:  
<http://www.ag.state.mn.us/consumer/Privacy/default.htm>

Federal Trade Commission:  
<http://www.consumer.gov/idtheft>

U.S. Department of Justice  
<http://www.usdoj.gov/fraud.htm>

Social Security Administration  
<http://www.ssa.gov/pubs/idtheft.htm>

Identity Theft Resource Center  
<http://www.idtheftcenter.org>

Fight Identity Theft  
<http://www.fightidentitytheft.com>

Identity Theft Protection by Promisemark  
<http://www.identity-theft-protection.com>

### Internal Contacts

Allina Legal Department  
612-775-5862

Allina Corporate Compliance Department  
612-775-5868

Allina Integrity Line  
1-800-472-9301

Allina Employee Assistance Program  
1-800-531-5145

Allina Human Resources Service Center  
952-992-8099 (local)  
1-877-992-8099 (toll-free)