Identity Theft: Policies and Prevention
by Tricia Jack, MPA, CPPA Research Associate

The act of assuming another person’s identity has been around for many years, but recently, identity theft has emerged as a huge problem for law enforcement agencies, government, business, banks and other financial institutions, as well as unsuspecting members of the public. This article seeks to explain what identity theft is, discuss Utah’s policies and legislation, and recommend ways to avoid becoming a victim.

Identity Theft: A Definition

Identity theft happens when an individual obtains personal information of another individual with the intent to impersonate them. It involves securing pieces of personal information such as social security numbers, birth certificates or driver’s licenses. Because the chances of being caught are much less than other crimes, it is becoming the crime of choice. It is the fastest growing crime in the U.S., to the extent that many police departments are overwhelmed with it and, therefore, some victims can’t even get a police report number, making it impossible for them to get any help.

How big is the problem in Utah?

The Federal Trade Commission reported that in 2006, it received 1,577 complaints of identity theft in Utah, representing 61.8 complaints per 100,000 population (Federal Trade Commission: Consumer Fraud and Identity Theft Complaint Data, February 2007). The Utah Attorney General’s website claims that as few as 33% of identity theft victims ever report the crime, so the extent of the problem is much bigger than what is reported. According to Kirk Torgensen, Deputy Attorney General for Utah, the explosion of identity theft in Utah is partly due to the meth problem, as a significant percentage of criminals are meth addicts.

What is being done in Utah to address the problem?

Utah is using a variety of methods to address the problem, including an award-winning identity theft website, legislation on credit freezes, criminal code amendments and a 2007 Senate Concurrent Resolution.

Identity Theft website

HB 432, signed into law in March 2007, requires the Utah Attorney General to maintain a website to assist victims of identity-related crimes. The website must allow victims to report the crime and have the report routed to the appropriate law enforcement agency. The website gives identity theft victims step-by-step instructions about how to repair their credit and protect themselves in the future. Victims also have access to sample letters and other documents to help them repair their credit. The website was recently honored through an award from the National White Collar Crime Center. It can be accessed at www.idtheft.utah.gov

Credit Freeze

SB 71 (passed and signed into law in 2006) allows a consumer to place a security freeze on their credit report. “If a security freeze is in place, a consumer reporting agency may not
release a Consumer’s credit report, or information from the credit report, to a third party that intends to use the information to determine a consumer’s eligibility for credit without prior authorization from the consumer” (Utah Code 13-45-201). This law becomes effective September 1, 2008.

Other Legislation

Legislation was also passed in 2007 regarding special revenue funds for identity theft investigations (HB341) and permitting the Department of Workforce Services to disclose to an individual the suspected misuse of the individual’s personal identifying information (SB15).

Criminal Code Amendments

Utah has also recently amended its criminal code in relation to identity theft. SB 140, passed in 2007, modifies the definition of personal information, and provides that it is a felony of the second degree to fraudulently use personal information that results in injury to another person.

Senate Concurrent Resolution

The Utah Legislature passed S.C.R. 1 in 2007 which urges the United States Congress to pass identity theft and fraud legislation related to the intentional misuse of a Social Security Number by an individual or a company.

Future Issues

Information from the Utah Attorney General’s website claims that future legislation might address issues of personal information contained in some public court records, and businesses becoming more careful about protecting customer records and informing them of security breaches.

Avoiding Identity Theft

Most people do not realize how easily criminals can obtain personal information and steal an individual’s identity. At a recent American Society for Public Administration (ASPA) meeting, Kirk Torgensen, Deputy Attorney General for the State of Utah spoke on the prevalence and problems of identity theft, and gave advice on how to avoid identity theft.

- Be careful with your wallet and purse. Identity thieves prey on unsuspecting victims in, for example, the grocery store when these items are often left unattended for a moment. If they steal your wallet containing a lot of personal information, they can easily steal your identity.
- Mail theft is the #1 source of identity information for thieves in Utah, so ensure you have a solid, locked mail box or consider using a P.O. Box address. Never leave mail in the box with the red flag up; this just attracts thieves.
- Minimize the amount of mail containing personal information that comes to your home such as bank and credit card statements. Try using internet banking and online statements rather than paper statements. If you are using internet banking with a wireless connection, ensure that an effective security system is in place.
- Opt out of receiving unsolicited credit card applications, especially the ones that have your information already completed. It is advisable to call the companies you do business with and tell them not to send anything.
- Be careful about what you throw in your garbage. Shredding documents will help a lot, but be aware that cross-cut shredders are much better. Straight shredders create “jigsaw puzzles for meth addicts.”
- Regularly reconcile your bank and credit card statements. This will help you to spot any
fraudulent activity early on.

- Protect your debit card information, especially your PIN. Be aware that some debit cards are not treated like a credit card so you may not be protected. Ask your bank how it is treated.

- Be careful about responding to emails asking for personal information. They may look authentic but they are most often not. Remember that legitimate businesses do not send unsolicited emails asking for your information. If you are unsure, call and check. The latest scam is an email coming from the IRS advising of a tax refund but requesting verification of personal information.

- Check your credit reports regularly to look for information in your credit report that makes no sense, e.g., a credit card you never had, or an address where you never lived. Last year the federal government passed the FACT act which allows everyone to get a free credit report from each of the three credit agencies once a year. To access this, go to www.annualcreditreport.com - don’t go to the “free credit report” advertisements, some of which may be imposters.

Mr. Torgensen also mentioned three things to do if you think you are a victim.

- Call one of the credit agencies and get a fraud alert put on your account.
- Consider freezing your credit.
- Contact the Attorney General’s office for advice.