Identity Theft Briefing Paper [1]

Identity theft (also known as identity fraud or true name fraud) is one of today's fastest growing crimes. While it might appear that the true victims of this crime are the merchants and lenders who extend credit to the thief in another person's name, they are not alone – all consumers pay higher prices to offset these fraud losses, while the victims whose identities are stolen suffer greatly because of the loss of their good name.

What is Identity Theft?

The basic goal of the identity thief is to steal personal information sufficient to impersonate a victim, so as to obtain credit cards, loans, and other items of value in the victim's name rather than their own name. In many cases, it is a crime of opportunity – a wallet is stolen, information is picked up by chance, a statement is delivered to an unattended mailbox, or someone's social security number is posted on the Internet. In other cases, the thief purposely pursues people who are in the news – minor celebrities, award-winners, athletes, accident victims, etc. – to mine the available publicity and data for identifying information.

What Information Is Needed To Steal An Identity?

Surprisingly little information is needed to impersonate a victim. The magic keys to a person's identity are their name and Social Security Number. So many databases in our society are keyed to this number that once obtained, it is virtually trivial to pass oneself off as the victim. However, an accumulation of other information can serve equally well – current or previous address, birth date, telephone number, biographical information, occupation, employer… Once identifying information is acquired, it is straightforward to apply for loans and credit cards, make purchases, obtain additional information and credit reports, change addresses on existing accounts, open and close accounts, apply for new drivers licenses and other identification, obtain passwords – the list goes on and on.

What Are The Potential Consequences of Identity Theft?

Identity theft has always been used by crooks as a tool to commit other forms of fraud and embezzlement, but has been given a real boost by the widespread use of the Internet. Thieves apply for, and often receive, multiple credit cards, personal loans, automobile loans, checking accounts, and other accounts in the name of the victim. They run these accounts up to the maximum, and then fail to make payments. This is particularly easy to do very quickly over the Internet, given its automated nature and the inability to physically verify an applicant's identity. These fraudulent accounts can total hundreds of thousands of dollars. Once they are past due, collectors harass the unsuspecting victim for payment. At best, the victim is inconvenienced by these collection efforts; at worst, their entire quality of life is irretrievably destroyed – and they usually must go through an extended, costly, and painful process to restore their good name.

Protecting Consumers' Identity – For Businesses

Perhaps the most important step a business can take to prevent identity theft is to not use the Social Security number as its customer identification number. Other steps include ensuring that this number does not appear on any reports released to the public or to employees at large, educating employees on the importance of keeping personal information about themselves and customers private, verifying the identity of callers claiming to be customers, and scrubbing personally identifiable information from their web site.

Protecting Your Identity – For Consumers
There are several very useful web sites listed below that outline the steps you should take to protect your identity from thieves, as well as what to do to recover from this alarming crime. In general, preventive steps include not giving out personal information unless it is absolutely necessary to complete a transaction, protecting your wallet or purse from theft, shredding sensitive personal and financial documents, and periodically reviewing your credit report to catch suspicious activity. Recovery steps include contacting credit reporting agencies to put a fraud alert on your credit file, filing crime reports with law enforcement agencies, contacting the security departments of merchants listing unauthorized accounts, and, most of all, remaining persistent.

Resources

- The US Government's central identity theft information site, maintained by the Federal Trade Commission [2]
- US Department of Justice's site – a good range of resources [3]
- Privacy Rights Clearinghouse – substantial repository of white papers, resources, and links to other useful sites on this topic as well as privacy in general [4]

Groups audience:
Treasurer

Links
[1] https://www.cu.edu/treasurer/identity-theft-briefing-paper [2] https://www.ftc.gov/tips-advice/business-center/privacy-and-security [3] https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud [4] http://www.privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you