Identifying the Concept of Theft And How To Prevent It

Abstract

As technology continues to have an increasingly larger role in the everyday lives of Americans, the issue of identity theft has also become a prevalent issue. In order to counter the growth of this trend, consumers need to be informed of the different ways that they can best protect themselves from becoming a victim. As more Americans are made aware of the triggers of identity theft, such as carelessness with the disposal of unwanted documents, using one password for multiple sites, etc, all that an individual can do in his or her own power to give the individual the lowest chance of becoming a victim has been maximized. In addition to public awareness, with the help of anti-fraud laws that have been passed by Congress, coupled with constant improvements made to website securities, the number of identity theft cases in the United States can at the very least be held from rising.

Keywords: identity theft, fraud, prevention, protection

The Dilemma of Identity Theft in Our Contemporary Society

As technology continues to play an increasingly larger role in the lives of millions of Americans, there is also an increasing number of identity theft cases. As a result, many begin to question the safety of their private information online. Therefore, how can identity theft be prevented by consumers, organizations, and anti-theft agencies? In order to combat this growing issue, many studies have shown that identity theft can be limited by incorporating anti-fraud laws, educating online consumers on the ways in which identity theft occurs and how they can help prevent themselves from becoming a victim, along with keeping website securities up to date.

What is Identity Theft?

In 1998, Congress passed the Identity Theft Assumption and Deterrence Act, in which identity theft is given a precise definition within Section 1028(a) of Title 18. In this section, identity theft is defined as when a person:

…knowingly transfers or uses, without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity… (the Identity Theft Act; U.S. Public Law 105-318).

In light of the definition provided by Congress, identity theft can clearly be regarded as a serious offense. Unfortunately, this offense occurs much more frequently than it should. According to the Bureau of Justice Statistics, approximately 17.6 million Americans were victims of identity theft in 2014, while approximately 16.6 million were victims in 2012 (Figure 1). Given this data, the rate at which the identity of Americans is stole is increasing by 500,000 citizens annually.

Once more, what makes identity theft frustrating is that it is quite difficult to catch a perpetrator

in the act of stealing someone's identity. As stated in a CBS article written by Rome Neal in March 2002, law enforcement agencies have found that credit card companies are rarely willing to work with law enforcement to help prosecute suspects of identity theft. Besides credit card companies' unwillingness to help, identity theft cases are not top priority for law enforcement, especially since cases of this sort require a considerable number of resources. In addition to their low priority, some cases of identity theft include a perpetrator that resides outside the victim's country of residence. As a result, this requires collaboration amongst police departments overseas, which is not an easy task (Neal, 2002). Towards the closing of the article, Neal interviewed Stephen Massey, an Oregon federal prison inmate, during which Massey stated that credit card companies need to tighten the screening process for credit card applications to help reduce the number of identity theft cases. During his time as an identity thief, Massey acquired $400,000 with an astounding 800 victims along the way (Neal, 2002). Given the above statistics, along with the personal perspective of an identity thief, the dangers of identity theft come in many different forms, of which consumers should be cognizant of.

How Does Identity Theft Occur?

The four most vital pieces of information for an identity thief is an individual's name, home address, social security number, a bank account number. A thief may not be able to obtain all four pieces, but other personal information such as a date of birth may be stolen instead. In today's contemporary society, there are three main forms of identity theft. The first and also most common form of theft is an individual's financial identity. This form of identity theft is most widely known because the reason for stealing such information is to purchase items at the expense of the victim. This is typically carried out by either opening credits card in the victim's name, or draining the money saved in his or her bank account (Norum, 2007). The second form of identity theft is criminal identity theft. In this form of theft, a criminal will pose as the individual whose information they have stolen, which ultimately frames the victim for the crime that the identity thief committed (Norum, 2007). The third and final form of identity theft is identity cloning, which is often the most detrimental to the victim. In this form, the perpetrator steals the vital pieces of an individual's personal information and uses it to start a completely new life (Norum, 2007). In most cases, the perpetrator will steal the identity of a young child because most parents fail to have their child's identity monitored to ensure that it has not been stolen. As a result, the stolen identity can go unnoticed for almost twenty years, or until the child starts to develop their own financial status.

Considering the numerous paths a perpetrator may take to steal an individual's identity, these paths can be boil down to two different methods. The perpetrator may use technology to facilitate the stealing of personal information, or they may search for tangible items that could provide them with personal information. Regardless of which method is used, identity thieves are equipped with a variety of tactics to steal personal information. Prior to incorporation of technology into the daily lives of Americans, perpetrators stole identities by searching through the trash of a given household in hopes of finding personal information on junk mail, or pieces of mail that should not have thrown out (Haygood, 2006). Additionally, identities were also stolen when lines formed at ATM machines, as a perpetrator could look over the shoulder of the person using the ATM while inputting their PIN number to gather personal information. Another method used to steal someone's identity, which is still used today, is a direct conversation with the potential victim (Haygood, 2006). Often done over the phone, a perpetrator will pose as a government official, or as a financial advisor from a local bank and ask for the verification of

personal information. Although this was a more prevalent method years ago, these approaches are still used today and unfortunately still work as well.

Besides the traditional methods used by identity thieves, perpetrators are also taking advantage of the increasing role that technology plays in the lives of Americans. The most common device used amongst identity thieves is a “skimmer” (Alberecht, 2011). The device is used to collect personal information from machines that an individual would use to swipe their credit card. A skimmer works identically to the machine that processes an individual’s credit card, but rather than sending the information to a bank, the information is fed directly to the perpetrator. Examples of such machines that are targeted by identity thieves are ATM machines and gas pumps because their location is often accompanied with very little, or sometimes no security. As a result, perpetrators can freely use skimmers on ATM’s and gas pumps during off hours and obtain credit card information from potentially hundreds of users.

A second technological method used by identity thieves is “phishing.” This particular method allows the perpetrator to dramatically increase the volume of potential victims, as “phishing” consists of sending a mass email, of which contains a link for the recipient to click on. Though the actual content of the email can vary, the main goal of the email is for the recipient to succumb to providing their personal information to a source that seemed to be legitimate. The same principle applies in the act of “SMSishing,” during which a text is sent asking the victim to confirm, or update their personal information. These two methods often yield successful results because of the perpetrator’s strategic use popular companies that the average person uses regularly. As a result, the victim can be easily deceived.

A third and final technological method used to steal the identity of a large number of people is hacking. As an increasingly popular trend, the network security of companies is constantly being upgraded or patched in order to close up possible “loop holes” in the system. Hacking is a process during which a perpetrator(s) attempts to bypass the security of a company’s system in order to gain access to a mass amount of personal information. This method has become a common practice among identity thieves due to prior cases of success that hackers have had. For example, in 2011 a hacker had successfully hacked into Sony’s network and had gained access to approximately 77 million users personal information including names, addresses, usernames, and passwords (Baker & Finkle, 2011). Although hacking into a company’s network is seldom an easy task, the volume of personal information than could be compromised for doing so serves as motivation for hackers to “crack the code.”

Recognizing that there are countless computer savvy individuals that attempt to break into online networks on a daily basis, one may question the level of experience necessary to successfully hack into a network. In an online article from Ars Technica, author Nate Anderson discusses how he became a password cracker. With no applicable experience, Anderson was able to crack approximately 8,000 passwords in just one day with the help of online research (Anderson, 2013). Considering this unsettling accomplishment, one may question the safety of their online information, given that an individual with no relevant experience in the field of password cracking was able to crack 8,000 passwords. In light of this particular article, the take home message for consumers is to educate themselves on the ways in which they can best prevent themselves from becoming a victim of identity theft.

Preventing Identity Theft

Although an individual cannot protect themselves 100% from becoming a victim of identity theft, there are a handful of approaches that can help minimize an individual's chances. First and foremost, an individual should be extremely careful with who they give their personal information to (Diller-Haas, 2004). Many of times over the phone, perpetrators will pose as a government official and state that he or she owes the government money and needs to confirm the potential victim's personal information in order to proceed. Often, these perpetrators target the elderly population, as they are typically the most vulnerable to caving into such scams. Besides being mindful to whom an individual discloses their information to, another approach for an individual to consider is to monitor their credit report on a yearly basis, at least. Additionally, there are numerous well-known companies that provide customers with identity protection services, like Identity Force (Diller-Haas, 2004). Although buying into companies such as Identity Force does reap clear benefits, it is important for companies to properly maintain their online security and notify customers in the event of a breach so that they can make changes to their accounts accordingly.

Another method to help reduce the chances of identity theft is to destroy unwanted documents that contain personal information. Although much soliciting of products is now received via email, junk mail that is simply thrown out may contain information that would be useful to a perpetrator searching through someone's trash (Alberecht, 2011). To avoid the issue, an individual should invest in a paper shredder to shred documents that have personal information on them in mass amounts to ensure that documents cannot be pieced back together. Also, an individual should be mindful to get their mail on a daily basis and not let it accumulate, given that packages, letters, etc are not secure in a traditional mailbox, especially since much of junk mail consists of credit card applications that are sometimes even preapproved. Therefore, an individual should collect his or her mail on a daily basis and shred unwanted documents. Times during which no one is home for an extended period of time, daily mail should be held at the post office to be picked up upon return to eliminate the possibility of mail being stolen.

A third approach to help prevent identity theft online is through the use of strong passwords. Often, people will create a strong password, but will make the mistake of using the same password for each website that he or she is a user of. On top of this mistake, some computers have software that will automatically remember and insert the username and password for each website if the user request that the computer remember their information. Should his or her computer be stolen, a perpetrator could be provided the information necessary to gain access to bank accounts and checkout information for online shopping sites (Fordham, 2008). Considering these repercussions, individuals should create passwords that contain upper and lower case letters, numbers, and special characters in an order that cannot be guessed. To remember usernames and passwords, a physical record should be kept in a private location. If an individual would like to take his or her internet security a step further, when prompted to provide answers to security questions, users should give illogical answers as a way to increase the security of his or her account.

In addition to the use of multiple strong passwords, it is also crucial for internet users to take further steps towards maximizing the security of their personal information online. In a world of which technology is constantly being updated, desktops, laptops, and handheld devices can often be deemed obsolete within five years of its release. As a result, when these devices are in need of repairs, it may be to the consumer's advantage to dispose of item and purchase a new one instead. In the event that a consumer does, the consumer should wipe the system of all personal information. To do so, the consumer can use a utility program, which is often build into

the device to overwrite the hard drive completely (How to Keep Your Personal Information Secure, 2012). However, during everyday use, consumers should be cognizant of conditions when he or she is providing their personal information. For consumers that partake in online shopping, he or she should be aware during the checkout process as to whether to not the website is considered to be a secure site. In other words, a “lock” icon is present to the left of the address bar on websites that encrypt your data during the checkout process (How to Keep Your Personal Information Secure, 2012). Besides the points of suggestion discussed, consumers can also use security software programs, such as Norton Anti-Virus. However, these programs are not substitutes for consumers to surf the web recklessly. In addition to using these programs, consumers should be conscious of their use of public Wi-Fi and keep his or her devices in a safe location when not in use. Despite the fact that no one can be 100% protected from identity theft, simple approaches such as those discussed can help reduce an individual’s chances of being victimized.

Conclusion

In light of the ways in which identity theft can become an individual’s nightmare, one may feel that becoming a victim of identity theft may be inevitable to avoid within a person’s lifetime. Although this statement cannot be rejected with a strong degree of certainty, there are numerous approaches that an individual should consider that will help reduce their risk. Hopefully, adopting such behaviors is enough to save individuals the hassle associated with being victimized by identity theft.