Identity theft research paper example

Business, Customers

Identity theft is something that occurs when a person uses another’s personal identity information, as his or her own. This personal information may include one’s name, credit card details, personal bank accounts etc. Using this information, the person who accesses this information can commit fraud and other illegal activity. Today identity theft is a very big problem throughout the world. According to the Federal Trade Commission (FTC), about 9 million Americans experience identity thefts each year. The criminals have plenty of opportunities to use the stolen identity and benefit. For instance the stolen identity may be used to obtain a credit card and you will not be aware of the theft until the bill reaches you.

Identity theft is the fastest growing type of crime in the US which also has the potential to jeopardize the country’s financial stability. About 9. 9 million Americans reported identity theft during 2008 which was about 22% rise from that reported in 2007. More recently as in 2011, about 12 million Americans had been affected by identity theft, which is actually a 13% increase from the previous year. The FTC estimates that consumers spend about $50 billion each year in costs due to identity thefts. Another important aspect of identity fraud is that it facilitates other crimes like employment fraud, document frauds, credit frauds etc that not only can affect an individual but also a nation’s economy and security. Policy makers have therefore taken identity thefts as a very serious issue.

There have been several legislative reforms to tackle identity thefts. The Congress has made identity theft a federal crime, even as early as 1998. Several legislations later followed to address aggravated identity theft. In its attempts to tackle this crime even further, Congress ordered the FTC to issue

an identity theft Red Flag Rule which ultimately became effective in June 1, 2010. The rule requires financial institutions and lenders to develop and have in place, identity theft prevention programs. In the US, several agencies including the FBI, Secret Service, Postal Inspection Services, Immigrations and Customs, and the Social Security Administration are involved in identity theft investigation.

Identity thefts have immense implications for its victims. While some identity thefts can be resolved quickly and easily, other thefts may require considerable amount of time and money. Some consumers may be treated unfairly or even denied loans and job opportunities due to their poor financial standing or credit history, which may actually be due to their identity theft.

Identity thieves use several ways to obtain personal information which include (Federal Trade Commission):

- Dumpster diving: Here the criminals looking for an identity to steal, search into the trash to get hold of any papers or documents that could have details of any person who would later become a victim of identity theft.
- Skimming: Here the fraudsters use skimmer device to get card information. These special storage devices retrieve and store the card information.
- Phishing: Here the fraudsters pretend to be representing a financial institution or a company and send spam or pop-up messages asking you to reveal your personal information like bank account login, secret numbers etc.
- Old fashion: This is an old method of stealing identity by which the information is got by stealing wallets and purses. Here the source of information from the owner gets into the custody of the criminal.

- Pretexting: By using false pretenses, the fraudsters get an individual’s name and personal financial information. For instance he or she may claim to be from a research firm and get personal financial details which are then used in the particular financial organization, acting as the person himself.

One of the most frequent and more invasive ways of fraudsters to steal identity is through hacking. Hacking is the unauthorized access and use of another’s computer systems, which has been a major cyber threat for the U. S. Hacking of an individual’s or an organization’s computer system has several implications for its associates and customers. A common way by which hackers get access to computer accounts is through a process called ‘ social engineering’ which include persuading individuals to release vital personal information to a stranger, through flattery, deception or intimidation (Ross, 2010). Once a hacker has access to the system, he or she is permitted to get all secret information and become capable of imitating the individual whose system had been hacked.

These identity thieves can use the stolen information to carry out several activities including:

- Opening bank accounts
- Obtaining credit cards, loans or other benefits
- Purchase or order goods in victim’s name
- Take control of existing accounts
- Obtain documents like driving licenses, passports etc under victim’s name.

The increasing globalization and the rapid growth or expansion of the Internet has made identification and apprehension of the identity thieves difficult. This is largely due to the fact that identity thieves can work across

geographical borders. It is therefore difficult to distinguish identity thefts committed by domestic criminals and international criminals (Finklea, 5-15). Also while some identity thieves work alone many others work in criminal networks or are a part of a larger crime syndicate. The FBI tracks down international criminal networks that steal and pass on identities to groups across the world, with their victims also scattered across the world.

Although identity thefts may be committed in several ways, the commission of an identity theft or the method by which it is carried out may be differentiated into the following stages (Newman, McNally):

Stage I (Acquisition) – Here the identity is acquired by any means including computer hacking, fraud, force or even through legal means like purchase transactions in the Internet

Stage II (Use) - The acquired identity is then used for personal gain of the fraudster, which includes not only financial gains, but also hiding one's original identity from law enforcement or other authorities. By hiding their actual identity, the criminals can evade arrest or other unfavorable actions. Sometimes the acquired information may also be sold in the black market. Additional identity documents like visas, passports, health cards etc. can be used for insurance frauds, stealing rented cars or even filing for tax refunds.

Stage III (Discovery) – Although the misuse of credit cards is known quickly, the realization of identity theft takes time. Sometimes it even takes about six months to a year to realize the theft. It has been established that the losses associated with an identity theft is proportional to the time it took for its discovery.

Despite the phenomenal rise in identity thefts, the management of identity

theft is yet to take off in a big way. Although the FTC has a huge database of identity theft complaints and victimization, the criminal justice system doesn’t have any national database reflecting the type and number of complaints reported, those solved or perpetrators persecuted. The FBI and Secret Services too have reported cases of identity thefts which again haven’t been broken down into an organized database at a state or agency level. Therefore it is impossible to determine the success of the criminal justice system in controlling identity theft. Unfortunately identity theft is a unique crime with several difficulties associated in reporting it. Three significant issues that hinder the reporting and recording of an identity theft as a crime are:

- Identity theft is difficult to be defined given its connections to other crimes. Several police departments do not have a provision to record or register identity theft as a separate crime. This is further made difficult by the fact that police officers are not trained in crime management of identity thefts.
- Identity thefts are generally of a cross-jurisdictional nature. The commission of the crime and its prosecution may span across varied jurisdictions. Despite significant efforts by the International Association of the Chief of Police Officials (IACP) to resolve this, there still exit many hurdles.
- Victims are likely to avoid reporting identity thefts to police. Depending on the type of the identity theft, they are likely to report the theft to banks, issuing authorities of credit cards etc. Therefore these financial agencies try and act to apprehend the culprits while addressing the victim’s problems. This aspect of reporting also discourages the police from taking a bigger role in tackling identity theft.

It is not just individuals, as even small business can fall prey to identity thefts. Just like individuals, companies and their directors too can fall prey to fraudsters. Similar to that happening among individuals, corporate identity thefts too can occur in several ways. This includes fraudulently changing the companies registration or ownership details, or entering into undesired transactions on behalf of the company or authorizing fund transfer from the companies' accounts. Fraudsters may also setup small, temporary companies offering products or services. Such companies are set up with an intention of committing fraud. They may also lure other businesses to make overpayments, whereby business organizations are later reimbursed excess payment by the fraudsters. Only when these fraud businesses declare bankruptcy and close down, do its customers realize that they had been duped (Action Fraud)

Information being important for businesses, the availability and confidentiality of that information is critical to their performance. On most occasions it is the information that drives any business, and client information is an important data for any commercial organization. Businesses often integrate this information through updations and movement of sensitive information which could include personal data, financial data, data on credit cards, addresses, personal records etc. whose security is very important and would have serious implications if breached. Given the fact that personal information of individuals is handled by organizations they deal with, they trust these organizations to ensure its security. Today we have sensitive documents including personal records, medical, legal and financial documents, transferred across shores, all

carrying with them the prospect of an identity theft. Companies like banks and financial institutions take data security precautions within their offices and headquarters, to thwart off efforts by hackers and intruders. However when relevant projects or processes are required to be outsourced overseas, these organizations have less control over the security of their data. They become fully dependent on the service provider to ensure data security for the information, which could include personal records. A lax attitude on the part of these organizations may prove costly for its customers. There have been reports of identity thefts on a massive scale from organizations and outsourced service providers.

The fear of identity theft may deter consumers from making easier and cheaper online options. They would also become wary of shopping for credit or spend considerably to protect their personal details (Anderson, Durbin and Salinger, 171-192). For businesses, preventing identity theft mean authenticating that buyers are actually the ones reflected by their identity. When creating new accounts, lenders rely on authentication of the individual. For accounts opened in person, creditors require photo identification or other physical proof of identity. However for accounts opened online, by phone or by mail, the proof is provided online, which the lender authenticates by comparing it to a third party database. This way identity thieves can impersonate a consumer by using stolen identity, through online application. Sellers and creditors employ several techniques to prevent frauds. The threat of an identity theft has driven many businesses and consumers to take precautions and include processes that are more expensive, but avoidable in the absence of this threat. Efforts to prevent frauds are also

costly for online merchants who require investing in fraud detection and prevention tools.

The development of technology is evident in every aspect of our lives, and one of the main changes is reflected in the way we communicate with each other. Computer Mediated Communication (CMC) has indeed redefined the way we communicate. Given the hectic life and the compulsions of the day, we have taken to the use of technology to communicate. CMC enables one to communicate either on a one-to-one basis or on a one-to-many basis. Despite several opinions on the effectiveness of technology in the way we communicate, no one can deny that that it has transformed our way of communicating. In the era of modern technologies, it is however very crucial to ensure the security of our personal information and its protection from identity thefts. It is also important to analyze the audience, distribution medium involved with the communication, the sharing practices, and access methods.

The rise of identity theft in recent times can be more attributed to the social media websites. Fraudsters look out for details like the date of birth, addresses and employment of individuals. Today the social media seem to have got everyone hooked to it. Social networking through social media websites has transformed the way people communicate and share with each other. Despite these facilitations, social media websites are a serious threat to individuals and organizations. The merits and potential of social networking can hardly be over stated. It must be mentioned here that social media sites are the most visited on the Internet and even the traditional media providers take to networking to deliver coverage and interact with the

audience. Although trust is an integral aspect of these websites like Linkedin, Facebook, Myspace, Twitter etc; they are very vulnerable to identity thefts. A recent report by Javelin Strategy & Research has indicated that in 2011, Linkedin had an identity fraud incident rate of 10% while it was 7% for Google and 5. 7% on Facebook (Waters).

Although public awareness about identity thefts is increasing, the number of such thefts also seems to rise. Despite newer technologies facilitating people in many ways, they also carry with them the prospect of offering new ways for identity thefts. People need to be more conscious to identity threats, particularly when transacting through the Internet or using the social media. Identity threat is something we will have to live with, but being alert and avoiding risks can provide a secure identity for each one of us.

Works Cited

Federal Trade Commission. “ About identity theft.” 2012. Web. 6 Dec. 2012.