



EVOLUTION OF IDENTITY THEFTS AND ONLINE FRAUDS ON INTERNET

Krishan Tuli*

Dr. Neenu Juneja*

Abstract: *As far back as the early 1990s, the Internet was argued to be a unique medium showing the fastest speed of diffusion in human history (Nguyen and Alexander, 1996). Today, there are very few people whose lives are not affected beneficially and/or harmfully by the technology of the Internet era. On the positive side, the ability to share and exchange information instantaneously has provided unprecedented benefits in the areas of education, commerce, entertainment and social interaction. On the negative side, it has created increasing opportunities for the commission of crimes – information technology has enabled potential offenders to commit large-scale crimes with almost no monetary cost and much lesser risk of being caught. Compared to perpetrators of traditional economic-motivated crimes (e.g., burglaries, larcenies, bank robberies), online fraudsters are relatively free of worry from directly encountering law enforcement and witnesses.*

Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in India. This article is based on various reports from news media and news portal.

Key words: *Cyber crime, Hacking, Phishing, Cyber squatting*

*Chandigarh Group of Colleges, Landran, Mohali



INTRODUCTION

As far back as the early 1990s, the Internet was argued to be a unique medium showing the fastest speed of diffusion in human history (Nguyen and Alexander, 1996). Today, there are very few people whose lives are not affected beneficially and/or harmfully by the technology of the Internet era. On the positive side, the ability to share and exchange information instantaneously has provided unprecedented benefits in the areas of education, commerce, entertainment and social interaction. On the negative side, it has created increasing opportunities for the commission of crimes – information technology has enabled potential offenders to commit large-scale crimes with almost no monetary cost and much lesser risk of being caught. Compared to perpetrators of traditional economic-motivated crimes (e.g., burglaries, larcenies, bank robberies), online fraudsters are relatively free of worry from directly encountering law enforcement and witnesses.

With the continuous advancement of Internet technology and personal computing devices in recent years, Internet crimes have risen to an alarming level. For instance, in the U.S., the National White Collar Crime Center reported a 33.1% increase in citizen complaints of Internet crimes between 2007 and 2008, and this figure is reflective particularly of the increased incidence of identity theft. Another source of information also indicated that the number of identity thefts increased more than tenfold within a 9-year period – growing from 31,140 incidents in year 2,000 to 313,982 in 2008. In addition, identity theft remained the top one complaint category filed by the victims across years. Evidence from victimization survey also pointed out that about 5% of Americans aged 16 and above was victims of successful and attempted identity theft within two years, and the direct financial damage to the victims were as high as 16 billion dollars. These statistics coincide with the notion of —Crime of the New Millennium— as the phenomenon quickly emerged in the 21st century.

On the basis of this upward trend, we aim to examine identity theft from an analytic angle with a focus on the expanded versatilities of this contemporary crime. In the present article, the mechanism of identifying an individual is first discussed, followed by the definition and typology of identity theft. Elements and methods of identity theft will be deconstructed for classification, and subsequent discussions will be emphasized on recent variations in online fraud. The study will conclude with the implications of the close relations between identity



theft and the fast growing Internet, and suggestions for improved means of identity protection.

PRINCIPLES OF IDENTIFYING AN INDIVIDUAL

The importance of identity can raise a series of scholarly discussions across disciplines. Decades ago, Erikson (1980) pointed out that the formation of identity is essential to individual development, especially during the period of adolescence. The term identity refers to the unique and stable characteristics associated with an individual, and the aspect of self is based upon the interior state of awareness. However, it is argued that the culture shaped by the modern information media alleviates the term from consciousness and associates with the body (Poster, 2006). The view introduced in the following sections probably evidences the shift. Admittedly, this perspective of identifying individuals may discard the psychological portion of identity but reflects an emerged culture in the digital era.

By the beginning of this century, computer geeks and security professionals had documented the application of three general principles of identity verification to protect user access to their personal belongings in the virtual space (Crume, 2000; Foster, 2005).

The **first principle** requires that a specific user knows some information to access the system, and the most visible example is a pair of username and password. Assuming the owners must have the knowledge of their identifying information this intuitive method has been widely adopted to guard numerous online services like paperless banking, email accounts, social-networking sites, interactive gaming, etc. Under some circumstances, occurred largely in the past, universally unique identifiers like Social Security numbers are used as IDs or method of verification, even though it is not really a —secure means to ensure the identity for an obvious reason: anyone who has the access to or the knowledge of the number(s) can pretend to be the person(s).

The **second principle** of identity verification is to have something in physical form such as a key, a document, or a smart card. Holding a passport when passing through customs and using a library card to borrow books are examples.

The **third principle** depends on what users must be biologically – which means using biological characteristics, such as the individual's fingerprints, voiceprint, iris, odor, and hand geometry – to verify their identity. This principle assumes that the chance of having



two different individuals sharing the same biological features is close to zero, the biological characteristics are realistically easy to measure, and the differences between biological information are practically detectable. The third principle is probably the most expensive of the three methods to execute due to the fact that obtaining another person's biometric information typically requires a higher level of technology and resources, including a fairly large information storage space and a measuring device. Meanwhile biometric verification provides the most secure protection to the owners because of its heightened technical thresholds.

Generally, combinations of the identifying principles provide a safer cyberspace for users, with a relatively higher level of security. With that increased level of security, however, comes a longer procedure for individuals to access personal belongings, and usually a higher service charge. The ATM card is a classic example of the combination of the first two identification principles — a user needs to present an ATM card (have something) and type in an access code (know something). This combination offers a greater degree of protection to property because more personal information is required. For the same reason, however, an extremely secure system that uses a combination of multiple identifying principles and employs advanced technology of the time is of limited use because of high associated costs. Collectively, our online property, ranging from personal information to —virtual wealth, is guarded by a system that is balanced (yet sometimes compromised) between the cost and the required security level.

THE U.S. LEGISLATION AND THE DEFINITION OF IDENTITY THEFT

Identity theft occurs when an individual obtains a piece of personal identifying information belonging to another individual and uses that information without the owner's knowledge or approval. The legal definitions of identity theft are usually more precise, but they vary from state to state. Perhaps a more well-recognized legal definition is the one from the U.S. federal legislation—the Identity Theft and Assumption Deterrence Act (ITADA).

ITADA of October 30, 1998, made identity theft a federal crime. Under this legislation, anyone who —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 commits a federal offense. Prior to the passage of this act,



identity theft was an element of many crimes, and law enforcement grouped its cases according to how the identity information was illegally used (General Accounting Office, 1998). Additionally, only the unauthorized use or transfer of identity documents was illegal under 18 U.S.C., while the unauthorized use of electronic access devices, such as credit cards, PINs, and ATM codes, was illegal under 18 U.S.C. 1029. The ITADA criminalizes the unauthorized use or transfer of a means of identification with the intent to commit or to aid or abet any federal violation or state felony. Since the passage of ITADA, the unauthorized use of credit cards is not only prosecuted under 18 U.S.C. 1029, but also falls within the ambit of 18 U.S.C.. Depending on the circumstances, the FBI, U.S. Secret Service, U.S. Postal Inspection Service, and Social Security Administration's Office of the Inspector General are the federal law enforcement agencies. Furthermore, it is important that states have their own laws to prosecute identity theft cases locally because the Act typically does not consider thefts below the \$100,000 threshold, most U.S. attorneys use to determine if federal prosecution should occur.

The Act satisfies a primary concern with the damages caused by the offense and delineates two types of direct and proximate harm of identity theft—harm to an individual's general reputation and his/her inconvenience. This Act also covers considerations of other damages, such as an undeserved poor credit rating that impedes job opportunities, or an inability to obtain financing. Simultaneously, the Act creates gaps for state governments to cover small-scale damages from identity theft and leaves holes of preventive actions, which will be addressed later. In 2004, the Congress passed another law named —Identity Theft Penalty Enhancement Act, in which the net is broadened to cover —new offenses of the time like terrorism and the severity of punishment is greater than before.

To facilitate the discussion in this manuscript, we adopted FTC's conceptual definition of identity theft. Specifically, we agree with that unauthorized possession of others identities guarantees fraudulent intentions, and in some cases leads to criminal consequences with financial damages. Treating these two terms as interchangeable or using them to segregate one episode into a series of illegal acts may generate unnecessary confusion. To a great extent, the contemporary conceptual scope of identity theft must highly overlap with identity fraud, if no other criminal activities are committed or facilitated by means of the



stolen identity. Under vast majority of circumstances, when obtaining another person's identity without authorization, the malicious intention is almost certain.

IDENTITY THEFT BREEDERS AND DAMAGES

Breeder identification can be gained by any means; its significance is in its use for obtaining additional, separate, false, or fraudulent means of identification controlled exclusively by the perpetrator without the victim's knowledge, or ability to know. An identity thief can fraudulently use obtained personal information to generate other means of identification, ranging from open new accounts, apply for loans and credit cards, to receive governmental benefits (General Accounting Office, 1998). Breeder ID means occur most often in the course of committing credit card fraud for the purpose of establishing the —authenticity required to obtain a new account, although their incidence is fairly frequent in conjunction with check fraud, document fraud/counterfeiting, signature forgery, and bank/loan fraud as well.

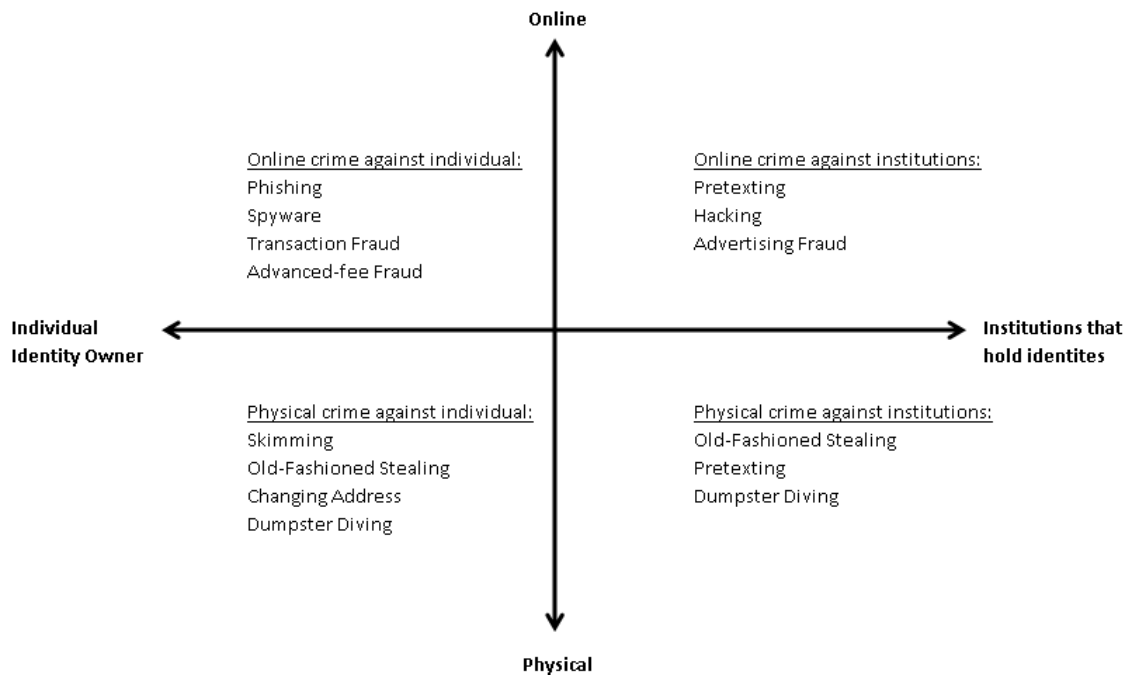
Thus, as long as the identity thieves have knowledge of or keep a record of the stolen identities, deeper and long-term damage to the victims can explode or surprise the victims at any time after the initial damage. For that reason, in addition to financial and credit damages, some victims of identity theft may suffer from varied psychological, social, and/or legal disturbances. These hidden costs are considerable but usually are not addressed. The recent supplement of the National Crime Victimization Survey shed some light in this regard – the emotional distress experienced by some types of identity theft victims (e.g., open new account, stolen personal information) were comparable to an average violent crime victim.

THE ELEMENTS AND OFFENDING METHODS OF IDENTITY THEFT

An identity thief may reach others identifying information through various means. The examples of identity theft are, probably, limited by each individual's imagination but expandable by the escalation of technology advancement. Here, we employ two dimensions to deconstruct the seemingly complicated incidents of identity theft.



Figure 1: Deconstructing Types of Identity Theft



The horizontal dimension is the source from which identity thieves obtain the identifying information. On one end of this dimension is the individual victim; on the other end are institutions that legitimately store client personal information. Stealing each individual's personal information generally is easier than penetrating institutions security protocols. However, once identity thieves penetrate layers of protection employed by those institutions, the loss of identity information is often massive and the damages are much more substantial.

The vertical dimension is the place where the identity-stealing conduct occurs. Identity thieves either violate social rules implemented in the physical world (e.g., steal individual victim's mails like bill statements containing personal information; bribe or coerce institutions employees who have access to clients personal information) or deceive Internet users of different services. Sometimes, the financial damage of identity theft does not begin until fraudsters purchase identity information that was collected illegitimately in the first place. The underground data warehouses that sell identity information online can contribute greatly to financial disaster for individuals.

The purpose of recognizing these two dimensions is threefold. First of all, these two dimensions help identify major dimension of paths that those identities are or can be stolen (cyberspace vs. physical space; individuals vs. institutions). The classification also lays out a



framework for detailed examinations of each type of identity theft. Without this foundation, further elaboration and analysis are limited.

Dumpster Diving/Trashing

Identity thieves can rummage through trash of residences or businesses looking for bills, paper documents, storage devices, and even discarded credit cards containing personal information. This way of stealing identifying information is fairly labor-intensive and is restricted to limited geographic areas. Consequently, suspects are relatively easy to locate by law enforcement agencies.

Old-Fashioned Stealing

Via traditional stealing methods, identity thieves either target goods that include personal information or obtain victims personal identification as a byproduct of pickpockets. The targets are those usually containing personal identifying information, such as wallets and purses, mail, especially bank and credit card statements, pre-approved credit offers, new checks, and tax information. Old-fashioned stealing can also occur when offenders steal personnel records from institutions or bribe/coerce/deceive employees who have the access.

Changing Address

Identity thieves divert victim's mail, particularly billing statements, to another physical location by completing a change of address form. This type of identity theft is usually conducted by filing the change-of-address form with the U.S. Post Office. Thus, the U.S. Postal Inspection Service is intuitively the corresponding law enforcement agency accountable for preventive/detering actions.

Skimming

Skimming occurs when legitimate transactions are processed by swiping credit/debit cards in retail stores or any other type of institutions where swiping cards is required. Generally, the credit/debit card numbers are stolen by a special storage device built in or attached to the swipe machines. The card information is stolen simultaneously when a legitimate business transaction occurs. The thief can be anyone who has access to the swipe machine, including, but not limited to, technicians of swipe machine vendors, and retail stores' staffs/owners. Skimming sometimes can be completed by perpetrators who attach a slim seem-like-real cover on a given ATM machine.



Pretexting

Pretexting involves a series of deceptive actions that obtain victim's personal information from the owner of the information, institutions that hold the information, and/or other individuals who may have knowledge of the information. Pretexters may pretend to have different roles (e.g., customer service representatives, survey researchers, the victims or the victim's authorized representatives) in order to collect pieces of victim's personal information. In sum, as a technique of social engineering, pretexting is a cluster of pretenses with the ultimate intention of taking financial advantage of the victims.

Hacking

Hacking was perceived as a creative activity that helped overcome the limitations of computers about a half century ago when such machines were not common, but the image of hacking changed, largely influenced by the media, to a threatening force in 1980s (Britz, 2009). The developed categories of hackers (e.g., white hat, black hat, and gray hat) are usually not mutually exclusive (McQuade, 2006; Parker, 1998) because whether their intention is malicious is uncertain from discovered evidence. Even though contemporary hacking is usually associated with stealing valuable information other than personal information (e.g., business secrets, confidential documents) and properties (e.g., copyrighted artifacts, billing) in cyberspace, it can be used as a means to obtain identifying information. Stolen identity information sometimes can be a —by-product of hacking for other purposes. Hacking is attractive for the reason that offenders do not have to physically appear at the —crime sceneto —rob or —steal from institutions. Instead, exploiting online financial and billing systems is enough to illegitimately gain privileged information. Especially after database technology is widely utilized by varied institutions to store and manage huge amounts of data, a copy of the database itself is very valuable in the black market. As more money, transactions, and even resources are moved to and managed in the virtual space for the sake of efficiency and convenience, it is likely hacking will remain a seductive means of identity stealing.

Phishing

Phishing is the pursuit of personal financial information with the intent to commit fraud by relying upon the recipient's inability to distinguish bogus emails, messages, web sites, and other online content, from legitimate ones – they all designed to appear with legitimacy.



Phishers can use a combination of tricks involving web sites, emails, and malicious software to deceive potential victims for the purpose of stealing their personal identity information and financial account credentials. The significance of phishing is that it enables remote identity theft. Precisely, phishing significantly reduces the risk and the costs to identity thieves because no physical contact, such as dumpster diving or old-fashioned stealing, is needed to complete the crime. Consequently, the chance of being caught at the crime scene is virtually eliminated. Another significance of phishing is its popularity in the U.S. where the largest proportion (25%) of phishing sites are hosted, compared to other countries in the world.

A typical phishing attack begins when phishers (offenders) send out massive amounts of email (spam) or messages with bait, which is intended to trigger the targeted victim's intuitive interests. Usually, the unsolicited emails ask recipients, with a sense of urgency often exaggerated by an alleged security breach, to log onto the provided URL and confirm their personal information details, particularly their password of access. Typically these fraudulent emails are designed to look like they are from large and well-known financial institutions, such as Bank of America, Citigroup, or PayPal. In the past several years, however, observers have witnessed that phisher's Spyware (Malicious Software).

ONLINE FRAUDS

In general, fraud refers to the act of taking advantage of others, largely motivated by economic reasons, via varied deceptive means. Online fraud intuitively refers to those conducted and/or facilitated by the Internet. As discussed earlier, identity theft is the inception of many fraudulent and criminal activities, but it does not necessary means that identity theft is the start of all online frauds.

Business Transaction Frauds

The network of computer networks creates a cyberspace where business transaction platforms, such as stores, can be operated virtually. In some cases, the same products demonstrated in a company's physical stores or printed catalogues can be found in their corresponding online stores. The most significant difference between buying from a physical or virtual store is the method of business transactions, including both the payment and the delivery of products or services, and this joint venue is where online frauds usually emerge.



Online Advertising Frauds/Advertisement Click Frauds

Cyberspace has created new business models, as well as new ways to advertise. One of the most common, and probably the least intrusive forms of advertising online is a banner on Web sites that invites interested customers to click on it and view the details. Once an Internet user clicks on the banner, s/he is linked to another site of products/services and the information system automatically records the click for later cumulative counts. The corresponding business model for charging the advertising fee is typically based on how many times the banner was clicked. Consequently, a particular fraudulent behavior online is to defraud Internet advertising billing systems by employing individuals or software to massively click on the advertisements. Outsourcing the task of fraudulent massive clicks to countries with cheap human labor becomes a rational choice to offenders.

Advanced-Fee Frauds

Advanced-fee frauds, again, is not something new in civilized human history, but this type of fraud has regained attention for its rapid increase use of email. The latest version of this fraudulent form is frequently referred as Nigerian 419 scam, named after the Nigerian criminal code section (Edelson, 2003). Online advanced-fee frauds generally begin with the receipt of a fake formal letter claiming a large amount of money needs to be transferred through a third-party bank account.

CONCLUSION

Identity theft and online frauds are contemporary crimes for profit. As the world market continues to progress toward transferring and managing money conveniently on the Internet, online frauds and scams are inescapable. As long as identity theft and online frauds are relatively easy paths to financial gain, the use of these fraudulent means will increase with the growth of the Internet. With the movement of processing transactions totally online, online fraud has gradually transformed from a hybrid cybercrime to a true cybercrime. Collectively, cyberspace has become such an attractive place where suitable targets like personal information increase in value while effective guardians typically fall behind. Anti-fraud efforts must be accelerated and orchestrated proficiently to make online scams difficult for offenders.



REFERENCES

1. Crume, J. (2000). Inside Internet Security: What Hackers Don't Want You to Know. Harlow: Addison-Wesley.
2. Cukier, W. and A. Levin. (2009). Internet fraud and cyber crime. In Frank Schmallegger and Michael Pittaro (ed.) Crimes of the Internet. Upper Saddle River, NJ: Pearson Education Inc.
3. Economic Crimes Policy Team (1999). Identity Theft: Final Report. United States Sentencing Commission.
4. Albert, M. R. (2002). E-buyer beware: Why online auction fraud should be regulated. American Business Law Journal, 39(4): 575.
5. Britz, M. (2009). Computer Forensics and Cyber Crimes: An Introduction. Upper Saddle River, NJ: Pearson Education Inc.
6. Federal Trade Commission. (2003). Overview of the Identity Theft Program: October 1998 – September 2003. [online]. Available from: <http://www.ftc.gov/os/2003/09/timelinereport.pdf> [Accessed 28/08/2010].
7. Federal Trade Commission. (2009). Consumer Fraud and Identity Theft Complaint Data: January – December, 2008. [online]. Available from: <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf> [Accessed 20/08/2011].
8. Federal Trade Commission. (2010). Consumer Fraud and Identity Theft Complaint Data: January – December, 2009. [online]. Available from: <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf> [Accessed 20/08/2011].
9. Huang, W. & Wang, S. K. (2009). Emerging Cybercrime Variants in the Socio Technical Space. In B. Whitworth & A. de Moor (ed.) Handbook of Research on Socio-Technical Design and Social Networking Systems. Hershey, PA: Information Science Reference, IGI Global.
10. Jasper, M. C. (2002). Identity Theft and How to Protect Yourself. Dobbs Ferry, NY: Oceana Publications.