Internet Journal of Criminology © 2011
ISSN 2045-6743 (Online)

THE EVOLUTIONAL VIEW OF THE TYPES OF IDENTITY THEFTS AND ONLINE FRAUDS IN THE ERA OF THE INTERNET

By Shun-Yung Kevin Wang and Wilson Huang[1]

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.

The authors 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.

[1] Dr. Shun-Yung Kevin Wang, Assistant Professor of Criminology, University of South Florida St. Petersburg, USA and Dr. Wilson Huang, Professor of Criminal Justice, Valdosta State University, Valdosta, USA

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 (2008, p. 2) 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 (Federal Trade Commission, 2009). In addition, identity theft remained the top one complaint category filed by the victims across years (Federal Trade Commission, 2009, 2010, 2011). Evidence from victimization survey also pointed out that about 5% of Americans aged 16 and above were 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 (Bureau of Justice Statistics, 2010). These statistics coincide with the notion of "Crime of the New Millennium" as the phenomenon quickly emerged in the 21st century (Hoar, 2001; Poster, 2006).

As crimes have advanced with technology, the breadth of online services and the number of users have continued to increase. We have witnessed that the Internet has made users' lives easier and has begun to link together varied segregated services (e.g., tele/communications, banking, investing, pharmacy, social interaction, education, entertainment) and devices (e.g., computers, servers, smart phones, even electronic chips in individual household air conditioning). The integration of such diverse technological applications coupled with the rapid growth of online users make fraudulent activities likely to rise further, if no intervention is proposed and implemented.

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 individuals' 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 users' 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. 1028(a)(1)-(6), 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. 1028(a)(7). 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 (Watkins, 2000).

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.

Since the passage of the ITADA, the official definition of identity theft has not changed much over the past decade. In addition, the Federal Trade Commission (FTC) was mandated by the Act to collect reported identity theft complaints, maintain the victim complaint database named the Identity Theft Data Clearinghouse, develop educational materials, and disseminate information (Federal Trade Commission, 2003). Thus, the oft-cited official definition, among widely varied state legislation, is the one posted on the FTC web site, and by 2011, FTC defines identity theft as:

> *"… occur when someone uses your personal identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes."*

By this definition, an incident of identity theft begins when an individual's personal information is stolen or transferred with an intention to commit other illegal and fraudulent activities. In some literature, however, identity theft and identity fraud are either interchangeable or completely separated. McNally and Newman (2008: 2) documented that: "Historically, identity fraud was viewed as being committed against the collective bodies (e.g., governments, financial institutions) that received fraudulent personal information rather than against the people who were fraudulently identified by that information. The term identity theft, which did not appear until the late 1980s, was initially used to distinguish individual victims (identity theft) from collective victims (identity fraud)……More recently, these terms have been applied in a different manner to separate the act of acquiring an individual's personal information (identity theft) from the act of misusing that information (identity fraud)." Britz (2009: 119), at the other end, argued that identity fraud ("a vast array of illegal activities based on fraudulent use of identifying information of a real or fictitious person") encompasses identity theft ("the illegal use or transfer of a third party's personal identification information with unlawful intent").

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

Identity thieves may not only gain immediately from committing frauds or other crimes against properties but may also "breed" further identities after initially obtaining

victims' identifying information. The context of this term "breed" refers to the unauthorized use of identification means to generate and/or acquire additional fraudulent means of identification.

"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). Studies have pointed out that driver's license, Social Security number, and birth certificate were most frequently used to "breed" other fraudulent identification means (Economic Crimes Policy Team, 1999; McNally and Newman, 2008; Slosarik, 2002). "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" (Economic Crimes Policy Team, 1999: 12). Possible harms may include transaction fraud, telecommunication services stealing, electronic funds transfer crime, electronic money laundering, and so on.

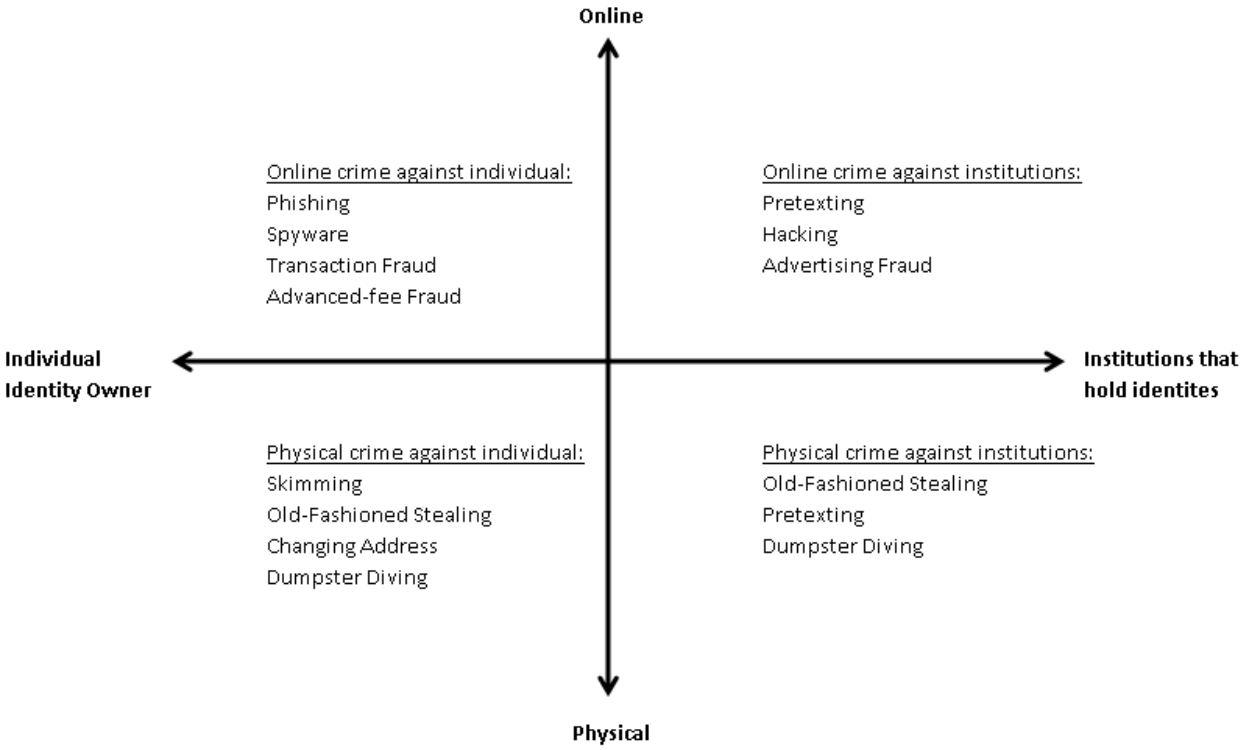
By abusing illegitimately obtained identifying information, an identity thief often commits fraud and gains financially through different paths as soon as s/he can. Less commonly, an identity thief may interfere with law enforcement by providing another person's identity upon arrest or during a criminal investigation or pull-over (Identity Theft Resource Center, 2003; Jasper, 2002), which is classified as secondary identity theft victimization by McQuade (2006). Under some extreme circumstances, victims of identity theft may suffer from being suspects of serious violence (e.g., murder) committed by identity thieves who un/intentionally leave the identifying means at the crime scene.

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 (Bureau of Justice Statistics, 2010).

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 clients' 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 (Symantec, 2007).

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. Next, after understanding how

identity thieves (can) obtain identifying information, law enforcement agencies, institutions, and individuals are better equipped to discover incidents, fix the emerging damages, and even prevent victimization down the road. Lastly, from the sorted identity-leaking paths, varied preventive strategies and actions (Marron, 2008; White and Fisher, 2008) can subsequently be implemented, and issues of effectiveness and accountability are thus better assessed.

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 "by-product" 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 victims' 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/deterring 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 victims' 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 victims' authorized representatives) in order to collect pieces of victims'

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 scene" to "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 (Britz, 2009; McQuade, 2006; Wall, 2007). 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 (Stroik and Huang, 2009).

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 victims' 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 (Cukier and Levin, 2009). In the past several years, however, observers have witnessed that phishers'

strategies have shifted from targeting banks to smaller financial enterprises, which increases the pool of potential victims.

Table 1 shows a sample of phishing sent to PayPal customers requesting their updated account information, and the message was received by one of the authors of this article through his personal email account. In the email, the company logo, division affiliation, and a clickable link are displayed professionally. The message, supposedly written by the PayPal support team, warns the customer that a violation against PayPal policy has been found. It threatens that if action is not taken promptly, a penalty including account limitation and even legal sanctions may be imposed. Though the email looks real, it has a redundant word, "multiple." It is quite common in phishing emails to find such syntax and/or grammatical errors which are extremely rare in formal letters from institutions. That is, errors in the writing can be viewed as indicators of fake letters from phishers.

Table 1: An Example of Phishing E-mail

Date: Wed, 09 Sep 2009 06:21:13 -0500
From: "support@paypal.com" <support@paypal.com>
Reply-To: "support@paypal.com" <support@paypal.com>
Subject: Paypal - Account Issue No.2819261

This is your official notification that your card has been limited.
We recently reviewed your card and it seems that it is linked to more than 1 accounts. Linking your Card to multiple accounts is strictly forbidden and it can be punishable by law. You are now requested to provide information relevant to your Card. Paypal will investigate the matter promptly and if the investigation is in your favor, we will restore your account.

* HOW CAN I RESTORE MY ACCOUNT ACCESS?

Click here [1] and complete the steps to remove limitations.

COMPLETING ALL OF THE CHECKLIST ITEMS WILL AUTOMATICALLY RESTORE YOUR
ACCOUNT ACCESS.

The Paypal Support Team
Please do not reply to this . Mail sent to this address cannot be answered.

Two contemporary variants of phishing—vishing and smishing, which utilize Voice of Internet Protocol (VoIP) and text messaging facilities respectively—emerged in recent years as the Internet was applied in telecommunications. Generally, vishing misuses Internet telephony's voice messages to facilitate the social engineering engagement with victims. The VoIP messages purport to be from banks and other financial institutions and deceive the recipients by advising that their credit cards or similar financial accounts have been used for fraudulent transactions. Those who respond to the call are requested to key into the phone their card numbers, expiration dates, three-digit security numbers typically shown on the backs of credit and debit cards, and maybe other personal information. In a similar vein, smishings use bulk text messaging facilities to target victims' mobile devices, such as cell phones, Blackberries, or PDAs. The phenomenon of vishing and smishing is partially attributable to the increasing failure of phishing attempts, resulting from a higher level of suspicion among general Internet users toward emails sent by financial institutions.

Another variant of phishing, pharming automatically directs recipients to the phisher's bogus Web site. Pharming is also known as "DNS poisoning," "cache poisoning," or "DNS spoofing." Unlike phishing, pharming does not rely upon social engineering to trick the recipient into clicking onto a Web site. Instead, it tricks the DNS by changing the targeted computer's stored records to convert domain names into numerical addresses. In other words, this trick "poisons" the computing devices through different ways (e.g., malicious software), instead of deceiving internet users.

Even though the average internet user has grown increasingly savvy, we continue to witness a substantial increase in phishing attacks. A recent report by RSA Anti-Fraud Command Center—an arm of the EMC Corporation, an international information security provider—indicated that within 2008, phishing attacks in the U.S. grew from just over 90,000 reported attacks to over 135,000 attacks, or a 66 percent jump (RSA, 2009).

Spyware (Malicious Software)

Unauthorized installed spyware can either keep a log of the victim's key strokes (e.g., usernames, passwords, security information) or actively seek out key financial information kept on the storage devices. The stolen information is then electronically sent to or retrieved by the offenders. Spyware has been used increasingly to steal personal information because the exponentially popular botnets that comprise lists of infected IP addresses can then be controlled remotely. It is also worth noting that the increasing sophistication of technology, particularly the blending of threats into one malicious software source, makes it increasingly difficult to distinguish identity theft from information theft and copyright piracy (Wall, 2007) —they are different aspects of a series illegitimate acts.

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.

In the era of the Internet, many existing frauds drive on this "information superhighway" and take advantage of the characteristic of anonymity in the cyberspace. Indeed, a good number of online frauds simply mirror existing frauds; others exhibit their uniqueness in this era. To distinguish the significance of online frauds, the coming discussions focus on those unique to the information age.

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.

Payment fraud can occur when fraudsters present a stolen, counterfeit, or cloned credit/debit card to purchase products from stores. This type of fraud is easier to carry out when verification is not a part of transactions, as is the case in online stores— nobody will (or, be able to) check customers' card information against their photos on ID! Moreover, the card information can be illegitimately obtained from different methods of identity theft (e.g., skimming, hacking) or purchased from other offenders who sell the card information that was illegitimately collected.

The other side of a given transaction involves the delivery of products or services. Fraudulent behaviors may include sellers' claims that they physically own the products or claims that they have delivered the products, when in fact they do not. Upon receiving the payment, fraudulent sellers disappear from the online transaction platforms (e.g., "close" virtual stores, withdraw from auction web sites). A sizable number of solved and unsolved legal cases demonstrates the easiness of abusing auction web sites as the means to carry out fraudulent intentions (Albert, 2002). Typically, "closing" online stores as a fraudulent method occurs to those that can be easily replicated and "re-opened" with different names familiar to potential victims.

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. The letter typically seduces potential victims with promises of a substantial proportion of the funds; however, an advanced fee must be wired to another account first in order to process the prerequisite works. To illustrate the methods of this scam, a sample letter gathered by one of the authors of this article through his email inbox is shown in Table 2. It can be found that the scammer claims to have control of the large fund and can distribute the fund to the recipient through an ATM card made for the recipient. Once the recipient receives the card, s/he is instructed to wire or send an advance fee to the fake bank for fund activation. But later, as the recipient attempts to redeem the card, s/he finds it be invalid. This lost to victims can be significant financially, psychologically, or even physically when the stakes escalate. If the process proceeds, victims may be asked to physically meet someone in Nigeria or other cities, followed by other forms of victimizations or another series of deceptive scam requiring more advanced-fees (Cukier and Levin, 2009).

Table 2: An Example of Nigerian Fraudulent E-mail

From: fmmrgovvrr00211@office.com
Subject: From: Former CBN Governor Very Important.
Date: Fri, 18 Dec 2009 06:56:20 +0100

HELLO, HOW/ARE/YOU/AND/YOUR/FAMILY?. HOPE ALL IS WELL.
How is your family today? I'm writing to notify you that I have successfully resigned as the Governor of Central Bank of Nigeria CBN, and this to inform you that your Contract/Inheritance Fund has been moved into Nigeria Treasure Account, while the accumulated interest of 2.5Million USD has been deposited with Intercontinental Bank Nigeria Plc.

I write to reveal this to you because I instructed the account officer in-charge (MR. EDWARD XXXXX) to load an ATM Master Card with the sum of 2.5 millions USD in your favor, as an interest Compensation to you. The ATM Card with its documents will be send to you via International Courier Service such as UPS or FedEx once you comply with the bank arrangement then the card will be send to you. In appreciation of the past disappointment you got from us during my time in Central Bank of Nigeria CBN as the governor.

The instruction was given to him on the 17th of November 2009, on my departure to Japan. Please contact the account officer with bellow contact information so that he can prepare the card and mail to you immediately once you come up with their requirement, The name of his bank is Skye Bank Plc. Contact him immediately.
Intercontinental Bank Nigeria Plc.
ATM Payment Department
Contact Person: Mr. Edward XXXXX
Tel: + 234 703 531 8213
Email: edwnkolepacenter011@gmail.com
Email: edwardbankole.cbnpayment.atmcard@gmail.com

Contact him with the bellow information immediately as well ask them the requirement for you to receive this ATM Card from the bank.
Your Full Name
Your address for deliver of your ATM Card
Your Direct Telephone Number both Mobile.

Let me know as soon as you receive the card so that we can rejoice together. Please my dear forgive me, it was too many commitment that caused the whole thing. Please accept my apology. I'm no longer the governor of CBN again, the republic retired me.
Thanks for forgiving me.
Best regard

Charles XXXXX
Former Governor, Central Bank of Nigeria.
Get Back To Me Once You Receive This Mail

Note: Personal names are replaced with XXXXX by the authors

Online Frauds and Identity Thefts

Online fraudulent acts committed by methods of stolen identification, phishing, advanced-fee schemes, or other electronic transactions fall largely within the arena of computer-assisted crimes (McQuade, 2006; Wall, 2007). Since the initiation of popularity of PC, computers have been used as instruments of fraud, and targeted for further crimes (Britz, 2009; Taylor, Fritsch, Liederbach, and Holt, 2011). Fraudsters resort to computers in either online communication to victims or financial transactions with banks. The computer is the main tool employed by online fraudsters to steal and store personally confidential information. Vulnerable Internet-connected computers usually turn out to be easy targets for hackers and botnet herders to harvest zombies. Perpetrators have utilized zombie computers and stolen email accounts to conduct spamming, phishing, and denial of service attacks. The impacts of these attacks can be devastating and long-lasting to individuals as described earlier; they can also be disastrous to institutions such as system collapse.

Though the majority of fraudulent activities are performed virtually without any physical contact between perpetrators and victims, the methods these crimes use are mostly executed offline. The Internet serves mainly as a medium for loading criminogenic elements and contents (e.g., phishing mail/link, Nigeria 419 letter, lottery winning notification) to facilitate the offensive intentions and actions of the perpetrator. As long as the Internet enables users to connect to others and to access belongings remotely, which is the strongest advantage of this technology, offenders will use the Internet to stay as far away from the "crime scene" as possible to avoid leaving biological identities like DNA—a mainstay of every episode of the extremely popular CSI television series. Regardless of the online or offline activities of the perpetrators, the computer is the key instrument and depository of their illegal acts. From the criminal justice standpoint, effective collection of digital evidence from the "crime scene" inside the networked computers is undoubtedly crucial to the solving of online frauds. On the side of Internet users, having a stronger security framework for the use and protection of identity information is probably most critical.

Filling the Gap between Using and Protecting Identity Information

At present, the majority of online activities use only the first identifying principle (*know* something) to confirm users' identities. Thus, obtaining an individual's username and password is often sufficient for a potential identity thief to masquerade as another person online. Some more sophisticated information systems probably request additional information that users should *know*, such as answers to security questions (e.g., what is your mother's maiden name?). However, this approach does not go beyond the scope of the first principle. Specifically, the level of security that guards varied properties and services in cyberspace is enhanced by increasing the *dosage* of the first identifying principle, not the *combination* of multiple identifying principles. It is suspected that the multi-dosage approach only slightly increases the security level because once identity thieves own the essential identifying information of others, secondary and further

identifying information, including answers to security questions, can be "bred" easily in the contemporary cyberspace.

Ironically, there is often a substantial imbalance between the value of guarded properties and the corresponding security level. For example, ATMs, which often cap cash withdrawals at $500 per day, use two identifying principles – *knowing* a PIN and *having* a debit or credit card – to guard our money. Online banking, on the other hand, uses only one principle – *knowing* a set of username and password – for transfers of thousands of dollars in matter of seconds. It is not saying that financial institutions do not have policies to screen transactions upon requests. But, the exceptionally low level of front-end protective means placed to guard properties stored in the cyberspace makes online accounts extremely attractive to offenders. In addition, because of such simplicity of online access, further illegal conduct like online frauds and credit damages can be simply done if a motivated offender successfully obtains victims' essential identifying information. For the same reason, it has been recognized, as early as the late 1990s, by law enforcement agencies that Internet growth contributes to identity theft-related risks (General Accounting Office, 1998; Lease and Burke, 2000). The recent escalating trend of identity theft and online frauds continues to echo the claim (Federal Trade Commission, 2011). Yet, not much has been done to fill this gap between our socially-based needs and protective technology capability (Huang and Wang, 2009).

Since accessing and managing money online has become more common among the general population, it is almost impractical to propose something that is against the existing trend. In addition, the trend has grown recently due to the environmentally friendly concept of paperless billing that online transactions provide. Many "green initiatives" will directly and indirectly increase the usage of the Internet for the ultimate purpose of decreasing the 'carbon footprint.' In the following paragraphs, we discuss several approaches as reasonable alternatives to the current practice of using and protecting identities online.

A number of approaches have been proposed and discussed to prevent identity thefts and frauds online. One notable approach is the situational prevention framework (Newman and McNally, 2005; White and Fisher, 2008), which stresses a reduction in opportunity for crime. The main idea behind this approach is that identity theft can be minimized if suitable targets are removed or well protected, potential perpetrators are monitored, and guardians exist. In other words, the removal of any one of three crime components can significantly decrease the chance of identity theft incidents.

Another significant discussion regarding identity theft prevention is the need for unifying laws. Uniformity at state-level legislation is argued as an important approach for two reasons. First, the consistency across jurisdictions between the state and federal levels will improve preventive and interceptive efforts. Second, the physical boundary of jurisdiction becomes less significant, if not unimportant, on the Internet. With unified laws and regulations, enforcement and prosecution efforts can be enhanced significantly with the assistance of the contemporary information technology. It is still anticipated that the trend of online identity theft will continue to grow, but a uniform state-level legislation and

model law together would be expected to lead to more efficient crime control (White and Fisher, 2008).

It is also worth noting that identity thefts targeting private corporations/institutions which hold personal information typically are not within the scope of protection addressed above. The IP Governance Task Force report (2006), has strongly recommended that a "red flag" be issued whenever precursors of identity theft exist. This approach particularly pertains to established institutions where potential losses from identity theft can only be prevented by proactive action at its inception. Given the knowledge that much greater damage can be done by "bred" identities in the long term, establishing different measures to signify financial institutions seems promising. Table 3 provides an example of FTC's announcement about scam emails that can victimize both clients (individuals and business) and governing agency.

Table 3: An Example of Announcement of Scam

Still another, and perhaps the most fundamental but not necessary the most welcome approach, is to increase the security level for accessing essential online property. With a broader and deeper utilization of the Internet in our daily lives, we foresee that cyberspace will "replicate" many more existed activities that already root in the physical world. A social-technical system of personal identity which grants a unique online identity for each resident may become an efficient alternative or even a necessity. To fundamentally protect the individual's rights online, administration should consider establishing a workable system that issues online IDs, similar to Social Security numbers, to each resident. In addition, this online ID has to be validated with a *combination* of identifying principles before a person can conduct activities in the *defined areas* in cyberspace. That means the infrastructure, including both hardware and software, has to be widely available at a reasonable cost, which is witnessed today. That also means, for a better collective good, Internet users have to sacrifice part of their "rights" like anonymity that they used to enjoy in the cyberspace. If such type of security system is successfully implemented, many other emerged issues of cybercrime (e.g., cyberstalking, child pornography and molestation, online gambling) can be greatly managed, too.

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

Albert, M. R. (2002). E-buyer beware: Why online auction fraud should be regulated. *American Business Law Journal*, 39(4): 575.

Britz, M. (2009). *Computer Forensics and Cyber Crimes: An Introduction.* Upper Saddle River, NJ: Pearson Education Inc.

Bureau of Justice Statistics (2010). *National Crime Victimization Survey Supplement: Victims of Identity Theft, 2008*. U.S. Department of Justice.

Crume, J. (2000). *Inside Internet Security: What Hackers Don't Want You to Know.* Harlow: Addison-Wesley.

Cukier, W. and A. Levin. (2009). Internet fraud and cyber crime. In Frank Schmalleger and Michael Pittaro (ed.) *Crimes of the Internet*. Upper Saddle River, NJ: Pearson Education Inc.

Economic Crimes Policy Team (1999). *Identity Theft: Final Report*. United States Sentencing Commission.

Edelson, E. (2003). The 419 scam: Information warfare on the spam front and a proposal for local filtering. *Computers and Security*, 22(5): 392.

Erikson, E. H. (1980). *Identity and the Life Cycle*. New York, NY: Norton.

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].

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].

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].

Federal Trade Commission. (2011). Consumer Fraud and Identity Theft Complaint Data: January – December, 2010. [online]. Available from: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf [Accessed 20/08/2011].

Foster, R. (2005). *Police Technology*. Upper Saddle River, NJ: Pearson Education Inc.

General Accounting Office. (1998). *Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited*. [online] Available from: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:gg98100b.pdf [Accessed 15/08/2011].

Hoar, S. (2001). Identity Theft: The Crime of the New Millennium. *Executive Office for United States Attorneys United States Attorneys' USA Bulletin*, 49(2). [online]. Available from: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm [Accessed 01/09/2011].

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.

Identity Theft Resource Center. (2003). *Identity Theft: The Aftermath 2003—A Comprehensive Study to Understand the Impact of Identity Theft on Known Victims*. [online]. Available from: http://www.idtheftcenter.org/idaftermath.pdf [Accessed 16/12/2010].

IP Governance Task Force. (2006). Comments on Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003.

Jasper, M. C. (2002). *Identity Theft and How to Protect Yourself*. Dobbs Ferry, NY: Oceana Publications.

Lease, M. L. and Burke, T. W. (2000). Identity theft: A fast-growing crime. *FBI Law Enforcement Bulletin*, 69, 8-14.

Marron, D. (2008). 'Alter Reality': Governing the risk of identity theft. *British Journal of Criminology*, 48: 20-38.

McNally, M. M. and Newman, G. R. (2008). Editor's introduction. In M. M. McNally and G. R. Newman (Ed.), *Perspective on Identity Theft*. Monsey, NY: Criminal Justice Press.

McQuade, S. C. (2006). *Understanding and Managing Cybercrime*. Upper Saddle River, NJ: Pearson Education Inc.

National White Collar Crime Center. (2008). *Internet Crime Report*. Washington, DC: Bureau of Justice Assistance, [online]. http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf [Accessed 02/09/2011].

Newman, G. R. and McNally, M. M. (2005). *Identity Theft Literature Review*. Paper prepared for the National Institute of Justice focus group meeting, Washington, D.C.

Nguyen, D, and Alexander, J. (1996). The coming cyberspace time and the end of polity. In R. Shields (Ed.), *Cultures of Internet*. London: Sage Publication.

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. New York, NY: Wiley Computer Publishing.

Poster, M. (2006). *Information Please: Culture and Politics in the Age of Digital Machines*. Durham: Duke University Press.

RSA (2009). *RSA Online Fraud Report*. [online]. Available from: http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_1208.pdf. [Accessed 16/08/2011].

Slosarik, K. (2002). Identity theft: An overview of the problem. *The Justice Professional*, 15(4): 329-343.

Stroik, A. and W. Huang. (2009). Nature and distribution of phishing. In Frank Schmalleger and Michael Pittaro (ed.) *Crimes of the Internet*. Upper Saddle River, NJ: Pearson Education Inc.

Symantec Corporation. (2007). *Symantec Internet Security Threat Report: Trends for January- June 06*. [online]. Available from: http://www.symantec.com/business/threatreport/archive.jsp [Accessed 01/09/2011].

Taylor, R., T. Caeti, D. Loper, E. Fritsch, and J. Liederbach. (2011). *Digital Crime and Digital Terrorism*, Upper Saddle River, NJ: Pearson Education Inc.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Malden, MA: Polity Press.

Watkins, M. D. (2000). Identity theft a nightmare, not impostor, in Internet age. *Police Chief*, 24: 26-29.

White, M. D. and C. Fisher. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review,* 19: 3-24.