

KEEPING ONE'S PERSONALITY AND HUMANITY IN THE ELECTRONIC AND CYBER AGE

KATLYN ANNE C. AGUILAR*

K

OUTLINE

- I. Introduction
- II. Concept of Identity Theft
- III. Legislative and Regulatory Responses
 - a. International setting
 - i. United States of America
 - ii. Singapore
 - iii. Canada
 - iv. China
 - v. Australia
 - b. Philippine setting
 - i. Bills filed in the 12th-14th Congress punishing computer and cyber fraud which incorporate identity theft
 - ii. Republic Act 8484

*11 LL.B., candidate, University of Santo Tomas. *Executive Editor*, UST Law Review.

iii. E-Commerce Act of 2004

iv. Executive Order 420

IV. Analysis and Conclusion

*“When the life of people is unmoral,
and their relations are not based on love,
but on egoism, then all technical improvements,
the increase of man’s power over nature,
steam, electricity, the telegraph,
every machine, gunpowder, and dynamite,
produce the impression of dangerous toys
placed in the hands of children.”
—the diary of Leo Tolstoy (1828 - 1910)*

INTRODUCTION

Before the existence of computers and other technological applications, human life has been restricted by their unavailability. The life of the common man of those times was not as luxurious as that of the modern times.¹

Among the products of the modern day technology are the internet and computer. Man gained easier and faster access to the whole world because of these. The proliferation of the use of internet has also given rise to Electronic Messages (e-mails) and Social Networking Sites (SNS). From the traditional mode of sending messages *via* mail, electronic message or e-mail has been an alternative mode for people. It further provided a more convenient and faster way of sending and receiving messages. Moreover, it has also been a means used in facilitating business transactions and negotiations easier.

Social network sites is a web-based service which enables individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system².

¹ <http://www.buzzle.com/articles/what-is-the-impact-of-technology-on-our-society.html> (last accessed Dec. 30, 2009).

² Danah M. Doyd, *Social Networking Sites: Definition, History and Scholarship*, <http://jcmc>.

Through these SNS, internet users have a means to connect with strangers with whom they share interests, political views and activities. These sites have also been considered as information and communication tools where blogging, photo and video sharing are possible. Among the popular social network sites are Friendster, Myspace, Facebook and Multiply.

A study was conducted by the Universal McClann to determine the countries with higher percentage of Internet users using social network sites. The study surveyed 17,000 internet users in 29 countries. The report indicated that 83 percent of Filipinos surveyed are users of a social network sites, making the Philippines the social networking capital of the world, followed by Hungary with 80 percent and Poland with 76 percent.³ It is estimated that nearly 90 percent of users in the Philippines have Friendster accounts.⁴

Meanwhile, the Philippines also ranks high in terms of specific usage of these social networks. The study estimates 90 percent of Filipino users read blogs, second only to South Korea (92%). Moreover, the Philippines also has the highest percentage of users (86 percent) that have uploaded photos in these social networks, ahead of China (73 percent), Mexico (72 percent) and Brazil (70 percent).⁵

Technology indeed has been considered as a boon to society. Nevertheless, not long before its existence, it has bred many unethical practices like hacking, spamming, phishing and identity theft. Among these practices, identity theft is becoming a major problem in the world, and the Philippines is no exception.⁶

indiana.edu/vol13/issue1/boyd.ellison.html (last accessed January 30, 2010).

³ *Philippines—The Social Networking Capital of the World*, <http://asia.cnet.com/blogs/infachat/post.htm?pid=63003580> (last accessed December 30, 2009)

⁴ Lawrence Casiraya, *RP has highest Percentage of Social Network Users- Study*, <http://newsinfo.inquirer.net/breakingnews/infotech/view/20080508-135336/RP-has-highest-percentage-of-social-network-users---study> (last accessed December 30, 2009).

⁵ *Id.*

⁶ <http://pinoyfranchising.blogspot.com/2007/07/philippine-identity-theft.html> (last accessed December 30, 2009).

Technology has gone far in affecting people's lives in this information age. Internet, nowadays, is fast becoming the alternative tool of fraudulent activities for economic or financial gain. With these, how far has our Philippine government, especially the legislature worked in combating the challenges of this age? Is it able to compete with its demands?

This article intends to explore the realm of identity theft in this information age, the measures undertaken by the international community and the state of preparedness of Philippine laws in deterring such act. It aims to illustrate the necessity of crafting an identity theft law in order for the government to be more enabled to compete in the information age.

CONCEPT OF IDENTITY THEFT

Identity theft is a type of consumer fraud and "occurs when a person knowingly uses another person's information in a fraudulent manner for the purpose of obtaining goods, services, or credit."⁷ The identity thief looks for information he can use to create official documents or gain access to financial accounts.⁸ The information obtained may be used to open a new credit card account or apply loans in the victim's name for his own use. Some pilfer bank accounts and illegally obtain professional licenses, passport, visas, driver's licenses and birth certificates.

Identity thieves use various methods of stealing personal information. These methods include but are not limited to:

- a. Getting information from businesses or other institutions by stealing records from their employer, bribing an employee who has access to these records, or hacking

⁷ Janice A. Alwin, Comment: *Privacy Planning: Putting the Privacy Statutes to Work for You*, 14 DEPAUL BUS. L.J. at 353, 357 (2002).

⁸ Martha A. Sabol, *The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?*, 11 LOY. CONSUMER L. REV. at 165, 166 (1999).

- into the organization's computers;
- b. Rummaging through one's trash, or the trash of businesses or dumps in a practice known as "dumpster diving";
 - c. Obtaining credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer, or someone else who may have a legal right to the information;
 - d. Stealing credit and debit card numbers as one's card is processed by using a special information storage device in a practice known as "skimming";
 - e. Stealing wallets and purses containing identification and credit and bank cards;
 - f. Stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information;
 - g. Completing a "change of address form" to divert one's mail to another location;
 - h. Stealing personal information from one's home; and
 - i. Scamming information by posing as a legitimate business person or government official.⁹

Nowadays, phishing and computer hacking are the most prevalent means of obtaining personal information. Phishing is a high-tech scam that uses spam or pop-up messages to deceive a person into disclosing his credit card numbers, bank account information, Social Security number, passwords, or other sensitive information. It is mostly done through an e-mail. Phishers send

⁹ Federal Trade Commission Report (2003).

an email or pop-up message that claims to be from a business or organization that you deal with Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that the person needs to “update” or “validate” his account information. It threatens some dire consequence if he does not respond. The message directs them to a Web site that looks just like a legitimate organization’s site. The purpose of this is to deceive a person into divulging his personal information so the operators can steal his identity and run up bills or commit crimes in his name.¹⁰

According to the January-June 2007 Internet Threat Security Report of software firm Symantec, a total of 87 percent of e-mails in the Philippines is spam. Richard Velasco, senior technical consultant for Symantec, said the high volume of spam is the result of spam “zombies” or computers infected with malicious software that send out thousands of junk e-mail everyday.¹¹

At present, phishing is also committed by means of social network sites. Users of SNS receive messages allegedly from the operators or owners of these sites requiring them to divulge certain information. Users are being threatened that failure to respond will result to inactivation of their existing accounts.

Sophos Asia-Pacific (Sydney), an IT Security Firm, in its study, revealed that Facebook is still a hotbed of identity theft.¹² Hackers lure users into taking actions they should not by making it appear as if a friend within their social network has sent them a message - only the message is from a hacker who has hijacked the friend’s account.¹³

¹⁰ Federal Trade Commission Consumer Alert

¹¹ David Dizon, *Cyber-crime Law Urgent, But Stalled in Congress*, <http://www.abs-cbn-news.com/special-report/06/06/08/cyber-crime-law-urgent-stalled-congress> (last accessed December 30, 2009).

¹² Tom S. Noda, *Facebook Still A Hotbed of Identity Theft, Study Claims*, http://www.pcworld.com/article/184522/facebook_still_a_hotbed_of_identity_theft_study_claims.html (last accessed December 30, 2009)

¹³ Carrie-Ann Skinner, *Beware: Identity Thieves Harvest Social Networks* http://www.pc-world.com/article/167511/beware_identity_thieves_harvest_social_networks.html?tk=rel_news (last accessed December 30, 2009).

Computer hacking, on the other hand, is more difficult to define. Computer hacking always involves some degree of infringement on the privacy of others or damage to computer-based property such as files, web pages or software. The impact of computer hacking varies from being simply invasive and annoying to illegal.¹⁴

Another trend in the modern world today is the use of credit cards in various dealings and/or transactions. It has been a preferred mode of payment for purchases of goods and services. The plethora of use of this form of transaction has engendered credit card offenses which caused financial burden to credit card holders and financial and banking industry. It has been a means in the proliferation of identity theft through the use of false, fictitious, stolen and lost credit cards.

The Philippines has been exposed to this problem for several years now. The Credit Card Association of the Philippines (CCAP) said that Philippines has the highest credit card fraud rate in the Asia Pacific, which is damaging the nation's image and tourism industry.¹⁵

EFFECTS OF IDENTITY THEFT

The effects of identity theft are as comprehensive as that of the means it is committed. It harms not just individual victims but financial and credit institutions or agencies as well.

The determination as to whether an individual is indeed a victim of identity theft is never an easy task nor an easy problem to solve. In most cases, the victim carries the burden of proving to lender or credit agencies that he did not personally incur the debit nor did he authorize the thief to use his name or credit to incur charges.¹⁶ Moreover, the victim has to take actions in

¹⁴ <http://education.illinois.edu/wp/crime/hacking.htm> (last accessed December 30, 2009).

¹⁵ Dennis Gadil, *Focus on laws curbing credit card fraud, Congress told*, <http://www.malaya.com.ph/may18/busi4.htm> (last accessed December 30, 2009).

¹⁶ Sabol, *supra* note 7, at 166.

order to repair his credit reputation and to clear his name with regard to the fraudulent transaction.

While the victim is attempting to correct the fraud, he is susceptible to further problems such as denial of education or housing loans. In some cases, he can be prosecuted and arrested pending the resolution of his claim.¹⁷ Rectifying an identity theft is an arduous process that entails emotional damage such as anger, hopelessness and frustration.

Financial institutions and credit bureaus, on one hand, endure the most in cases of identity theft. It is these institutions who suffer the economic losses brought about by use of fraudulent or fake identities. Credit card fraud has becoming more rampant that credit card companies are investing heavily on fraud detection and risk management tools, and recoup the additional costs through higher rates.¹⁸

LEGISLATIVE AND REGULATORY RESPONSE TO IDENTITY THEFT

Identity Theft in the International Level

The United States of America, as early as 1998, has promulgated a law that would deter the rising number of identity fraud. This is known as The Identity Theft and Assumption Deterrence Act (“ITADA”), which was signed into law in October of 1998. ITADA was the first comprehensive effort to rewrite the federal criminal code to address the effects of identity theft on individuals. Aside from defining identity theft as a crime, it has also recognized the consumer as the victim and provided specific remedies and penalties.

The ITADA made “it illegal to steal another person’s personal identification information with the intent to commit a violation, regardless of

¹⁷ FEDERAL TRADE COMMISSION, *ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME*, 1 (2002) at <http://www.ftc.gov/bcp/online/pubs/credit/idtheft/htm>.

¹⁸ *Id.* at 15.

actual possession of identity documents.” Further, it has directed the Federal Trade Commission to establish a centralized clearinghouse “to record and track complaints, and to provide consumer education service for victims of identity theft.” The FTC “was designated as a communications post, which receives victim complaints and educates consumers on prevention methods.”¹⁹

Despite these unique features of the ITADA, it failed to fully address the issues concerning identity theft. The law was not able to provide adequate legal remedies to victims such as the remedy of restitution of costs on accounts of victims of identity theft.

In 2003, another legislative measure was signed into law, the Fair and Accurate Credit Transactions Act of 2003 or FACTA. FACTA provides consumers, companies, consumer reporting agencies, and regulators with important new tools that expand access to credit and other financial services for all Americans, enhance the accuracy of consumers’ financial information, and help fight identity theft.²⁰ Further, FACTA provides several lines of defense to protect consumer’s account.

The act entitles a consumer to a free credit report once a year from each of the three major credit bureaus -- Experian, TransUnion, and Equifax. One is also allowed to put a fraud alert on his credit file so that lenders have to contact him before opening new accounts in his name.²¹

On the side of business establishments and entities, the act requires them to promulgate policies and regulations in dealing with sensitive information in order to thwart the risk of identity fraud. They are further required to look for “red flags,” such as address discrepancies or new charge card requests that are out of the ordinary and to dispose of records responsibly so they do not get in the wrong hands.²²

¹⁹ Alwin, *supra* note 6, at 353, 357.

²⁰ Robert Longley, *New Law to Protect against Identity Theft*, <http://usgovinfo.about.com/cs/consumer/a/idtheftbill.htm> (last accessed November 3, 2009).

²¹ *Id.*

²² *Id.*

Another line of defense which the law provides is the victim assistance. The law offers help to those who have already been victimized. It allows people with proof of identity theft, and proof that they are who they say they are, to get copies of the documents the thieves used to create false accounts. They can also block fraudulent information from their credit reports and get details on all debts being sent to collection agencies so they know if they are valid or not.²³

In line with the policy of the United States of America to avert identity theft, the Identity Theft Penalty Enhancement Act was signed into law in 2004. Unlike the ITADA and FACTA which directly provide measures to protect victims of identity fraud, the law merely provides harsher penalties for the crime of identity theft. It has introduced the crimes known as aggravated identity theft and terrorism-related identity theft. Aggravated identity theft occurs when the theft is used to commit another crime, such as buying stolen property or creating false identification. Terrorism-related theft is basically aggravated theft that involves a terrorist crime.²⁴

According to the law, thieves can get up to five years in prison for traditional identity theft, at least two years for aggravated identity theft, and at least five years for terrorism-related identity theft. They can also be punished for additional aspects of their crimes.²⁵

Singapore

Just like the United States of America, the Singapore legislature has enacted laws that deal with cyber-crimes and other computer-related crimes. Its principal law that responds to the growing number of these crimes is the Computer Misuse Act (hereinafter CMA) which was passed into law in the year 1993 and has been amended four (4) times, as recently as 2005. It was based primarily on the United Kingdom's (UK's) 1990 legislation of the same

²³ *Id.*

²⁴ <http://www.spendonlife.com/guide/identity-theft-laws> (last accessed November 14, 2009).

²⁵ *Ibid.*

name, but there are some divergences.²⁶

The CMA prohibits the obtaining of unauthorized access to computer material, modifying the contents of a computer, obtaining or intercepting any computer service or function, interfering with or obstructing the lawful use of a computer, impeding or preventing access to or impairing the usefulness or effectiveness of any computer program or data, or disclosing a password, access code, or other means of gaining access to a program or data.²⁷ It has given broad application in order to cover all forms of digital transaction and to effectively respond to the rapid changes in technology.

Aside from the broad coverage of the law, it likewise provides stiffer penalties to its violators. Most of the provisions of the Computer Misuse Act carry a maximum fine up to \$10,000 Singaporean dollars and/or imprisonment up to three years for the first offense. For the second and subsequent offenses, the penalty is a fine up to \$20,000 Singaporean dollars and/or imprisonment up to five years. If there was damage caused as a result of the crime, the penalty is a fine up to \$50,000 and/or imprisonment up to seven years. If the crime involved a threat to Singapore's security, or to the banking or other financial, communications, or transportation industries, or to public services including utilities, safety, police, civil defense, or medicine, the penalty is a fine of up to \$100,000 Singaporean dollars and/or imprisonment up to 20 years.²⁸ Further, the Penal Code provisions have been applied to activities considered as cyber-crimes. For example, the release of a virus would fall under the jurisdiction of the Computer Misuse Act, whereas an economic crime (e.g. extortion or securities fraud) would fall under the aegis of the Penal Code.²⁹

CMA signifies four approaches that are being used by the Singapore government to combat cyber-crimes. These are: a.) promulgation of laws

²⁶ Gregor Urbas, *An Overview of Cybercrimes Legislation and Cases in Singapore*, <http://law.nus.edu.sg/asli/pdf/WPS001.pdf> (last accessed December 30, 2009).

²⁷ <http://www.crime-research.org/news/01.04.2008/3286/> (last accessed November 14, 2009).

²⁸ *Id.*

²⁹ *Id.*

that punish cyber-crime; b.) providing harsher penalties in case of violation thereof; c.) creation of law enforcement agencies and providing them with extra-territorial jurisdiction and additional powers; and d.) punishing the abet and mere attempt to commit any act considered as cyber-crime.

Although the law does not directly make mention of identity theft, the commission of the said act is punished under it especially when the means employed was through the use of computers or other digital technology.

Singapore has a broad range of CMA offenses and others in the Penal Code and elsewhere, that serve to criminalize most known varieties of cybercrime. The abetment and attempt provisions of both the CMA and the Penal Code allow law enforcement officers to intervene at preparatory stages of crimes, and the extra-territorial scope of the CMA allows prosecution even where the preparatory conduct occurs outside Singapore.³⁰

Canada

Just like most nations in the world, identity theft costs in Canada have been greatly increasing for the past two years. According to Canada's largest credit reporting agency, 40,000 identity theft cases were reported in the past two (2) years. In 2007, more than 10, 000 victims reported losses of more than \$6 million to PhoneBusters, the Canadian anti-fraud call center. It increased to more than \$8 million in the first 10 months of the year. In addition, the Canadian Council of Better Business Bureaus has estimated that identity theft may cost Canadian consumers, banks and credit card firms, stores and other businesses more than \$2 billion annually.³¹

As a response to this growing problem of identity theft, Bill S-4 known as "An Act to Amend the Criminal Code (Identity Theft and Related Misconduct)" received Royal Assent and came into force on October 22, 2009. The Bill creates two new key offenses: the offense of "identity theft" which refers to the act of collecting an individual's personal information in

³⁰ *Supra note at 22.*

³¹ http://www.canadaone.com/ezine/briefs.html?StoryID=09Oct28_1 (last accessed December 30, 2009).

circumstances that give rise to a reasonable inference that the information would be used to commit an indictable offense and the offense of “identity fraud” which refers to the use of the information to impersonate a person.³² Specifically, the Act punishes the unlawful use of identity document, the false representation of a person as a police officer, the unauthorized use of credit card data, the trafficking of identity information and government-issued identity documents and the stealing of identity documents by means of mail.

Any person found guilty of any of the offenses mentioned in the Act shall suffer a penalty of imprisonment for not more than five (5) years or not more than ten (10) years or not more than fourteen (14) years, as the case may be. In addition to the penalty of imprisonment, the court may order the offender to recompense the victim.

The Government of Canada is committed to thwart any infringement of the privacy of its citizens. Aside from the newly-passed Bill S-4, it has also an existing law that aims to build consumer's trust and confidence in conducting e-business in Canada. This is the Personal Information Protection and Electronic Documents Act (PIPEDA) which came into full effect on January 1, 2004.³³

The provisions found in PIPEDA are based on the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), which has the following features:

1. Organizations are required to seek the consent of individuals prior to collecting, using or disclosing their personal information;
2. Organizations must protect personal information with security safeguards appropriate to the sensitivity of the information; and
3. Individuals may access personal information about themselves held by an organization and have it corrected, if necessary.³⁴

³² <http://www.dww.com/?p=1603> (last accessed November 09, 2009).

³³ http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00045.html (last accessed October 30, 2009).

³⁴ *Id.*

PIPEDA seeks to put a balance on the right of its citizens to privacy and the need of government agencies and institutions to collect and use personal information for legitimate purposes. Moreover, it provides a legal framework for the use of electronic documents in transactions as alternative to paper-based communications.

China

Identity theft is also prevalent in China. Although China has yet to enact a law that will directly punish identity theft, one does not enjoy total liberty to commit such crime. Certain provisions of the Chinese Criminal Law are being applied to punish perpetrators. Section 279³⁵ of the said law punishes the act of deceiving or misrepresentation as a State functionary. It is considered as government identity theft which is punishable by imprisonment of not more than three (3) years or imprisonment of not less than three (3) years but not more than ten years (10) years, if the fraud committed is serious.

Sections 280, 281 and 282³⁶, on one hand, cover non-governmental

³⁵ In full, it reads: Article 279. Whoever impersonates a functionary of a State organ to go about and deceive people shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights; if the circumstances are serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than 10 years.

³⁶ In full, it reads: Article 280 Whoever forges, alters, buys, sells or steals, forcibly seizes or destroys the official documents, certificates or seals of a State organ shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights; if the circumstances are serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than 10 years.

Whoever forges the seals of a company, enterprise, institution or a people's organization shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights.

Whoever forges or alters identity cards of citizens shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights; if the circumstances are serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years.

Article 281. Whoever illegally manufactures, buys or sells the people's police uniforms, number plates of police vehicles and other police insignia or police implements, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more

and individual identity fraud. These provisions punish the act of forging and altering seals and trademarks of companies and other agencies and passports, visas and resident identification cards. They likewise prohibit the illegal manufacturing, selling and buying of police uniforms, insignias and number plates of police officials. Moreover, an individual who possesses strictly confidential documents, papers and materials are required to explain their sources and purposes.

The same penal sanction as those of governmental identity fraud is imposed to violators of Sections 280, 281 and 282.

Despite the application of Chinese Criminal Law, the Chinese government cannot fully combat the growing number of identity theft. Section 279 of the law only punishes deceit by means of misrepresentation as State functionary. It fails to cover situations where a person misrepresents another to obtain personal and confidential information to derive personal benefits. With regard to Sections 280, 281 and 282, there is only limited application for they only cover seals, trademarks, passports, visas and resident identification cards. Moreover, since the acts being punished fall within the scope of Chinese Criminal Law, specific criminal prosecution is essential before one can be

than three years, criminal detention or public surveillance and shall also, or shall only, be fined.

Where a unit commits the crime mentioned in the preceding paragraph, it shall be fined, and the persons who are directly in charge and the other persons who are directly responsible for the offense shall be punished in accordance with the provisions of the preceding paragraph.

Article 282. Whoever unlawfully obtains State secrets by stealing, spying or buying shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights; if the circumstances are serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years.

Whoever unlawfully holds the documents, material or other objects classified as "strictly confidential" or "confidential" State secrets and refuses to explain their sources and purposes shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention or public surveillance.

prosecuted and convicted.³⁷

In order to respond to the growing number of identity fraud, the Chinese Government is on its way of crafting laws relative to identity fraud cases. Various proposals were made for the enactment of Personal Information Protection Law where the Personal Information Protection and Electronic Documents Act of Canada will serve as its basis.

Australia

Identity security is an issue of critical concern to Australian citizens, government and business. It is essential to Australia's security and economic well-being that the identities of people seeking access to government or commercial services, benefits, official documents and positions of trust, can be accurately verified in order to prevent the use of false identities.³⁸ Identity theft is also a major invasion of privacy and a high level concern in the Australian community.³⁹ Australia's financial agency and financial sector surveyed that in 2001-2002, a total of \$1.1 billion damages were caused by identity theft.

The Australian government recognizes the fact that the use of false, fraudulent and stolen identities underpins criminal activities and terrorism. In order to combat these problems and to protect identities of Australians from being used illegally, the government has introduced and undertaken various regulatory measures. These initiatives include: a.) National Identity Security Strategy; b.) The National Document Verification System (DVS); and c.) The ID Theft Booklet.

³⁷ Vicente Yang, Ph.D., *ID Fraud in China: Challenges and Options*, F:\Vincent Yang PhD- ID Fraud in China Challenges and Options.pdf (last accessed December 30, 2009).

³⁸ Council of Australian Governments Special Meeting on Counter-Terrorism, *Communiqué*, 27 September 2005, <http://www.coag.gov.au/meetings/270905/index.htm#Identity>, (last accessed December 30, 2009).

³⁹ Address by Karen Curtis, Privacy Commissioner at the Safeguarding Australia Conference, Canberra 12-14 July 2005 at http://www.privacy.gov.au/news/speeches/sp06_05.pdf (7 December 2006)

National Identity Security Strategy

The Council of Australian Governments (COAG) took into consideration identity security problems when it convened on September 27, 2005. COAG agreed to the development and implementation of a national identity security strategy, underpinned by an inter-governmental agreement (IGA), the development and implementation of a national document verification service to combat the misuse of false and stolen identities, and to investigate the means by which reliable, consistent and nationally inter-operable biometric security measures could be adopted by all jurisdictions.⁴⁰ The central element of the National Identity Security Strategy is the development of systems for verifying the integrity of key identity documents.

The enactment of Strategy aims to meet the following objectives: a.) improvement of standards and procedures for enrolment and registration for the issue of proof of identity documents (POI); b.) enhancement of security features on POI documents to reduce the risk of incidence of forgery; c.) establishment of mechanisms to enable organizations to verify the data on key POI documents provided by clients when registering for services; d.) improvement of the accuracy of personal identity information held on organization's databases; e.) enable greater confidence in the authentication of individuals using online services; and f.) enhancement of the national inter-operability of biometric identity security measures.⁴¹

In order to facilitate and advance the objectives of the National Identity Security Strategy, a coordinating body known as the National Identity Security Coordination Group was also established. This body is composed of representatives from central agencies of the Australian and State and Territory governments, the Council of Australasian Registrars for Births, Deaths and Marriages, Austroads and the Privacy Commissioner.

⁴⁰ http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity (last accessed December 30, 2009).

⁴¹ *Id.*

The National Document Verification System

The birth of the document verification system (DVS) is a product of a feasibility study conducted by the Australian government and agencies. The study found that POI processes could be significantly strengthened and registrations or enrollment of persons for high value transactions made less open to fraud if agencies were able to confirm the personal information appearing on key POI documents.⁴²

The DVS was then developed which allows authorized Commonwealth, State and Territory Government agencies to verify the details of documents presented to them as POI with the data recorded in the register of corresponding document issuing agencies. It determines whether proofs of identity submitted by a person are authentic, true and up-to-date. If a document “matches” information held by the issuing agency, a “yes” response is transmitted to the querying agency; otherwise, a “no” response is returned indicating that the document details were not verified. No personal data is transferred from the document-issuing agency. At present, passports, visas and driver’s licenses are among the proof-of-identity that can be verified using the system.

The use of DVS by various government agencies posed another responsibility for the reason that they were required to employ IT security measures in order to ensure that only authorized staffs will have access to the personal information. Moreover, in order to mitigate the risk of inappropriate invasion of Australian’s right to privacy, the Office of the Privacy Commissioner was tasked to craft a Privacy Impact Assessment (PIA) that will provide a framework in the implementation of DVS.

Identity Theft Booklet

Identity Theft is one of the recognized rising problems in Australia. In order to educate Australians on how to prevent and respond to identity theft, the government has prepared a booklet, distributed to its citizens, known as ID Theft Booklet. It provides practical strategies on how individuals can protect

⁴²*Id.*

themselves from becoming victims of identity theft, and what to do if they become a victim of this crime.

In addition to the efforts of the Australian government to educate its citizens, identity document issuers and government agencies are working together to improve the management of lost, found and stolen documents. These documents are commonly used by identity thieves in order to gain access to goods and services.

Australian states and territories have also taken individual actions in combating the problem of identity theft. These are reflected by their respective common and statute laws. Victoria, Queensland, Tasmania, Western Australia and South Australia were among the states which incorporated the crime of identity theft or identity fraud in their statutes.

In the case of Victoria, identity thieves are punished by applying certain provisions of Crimes Act of 1958 specifically Sections 81 (a) and 82. These two (2) provisions proscribe the taking of property and financial advantage by means of deception. Queensland, Tasmania and Western Australia likewise apply their respective criminal laws to punish identity theft perpetrators. Their criminal laws punish the act of gaining financial advantage by means of stealing false documents, record, information and data.

South Australia's Criminal Law Consolidation (Identity Theft) Amendment Act 2004, which amended Criminal Law Consolidation Act of 1935, specifically concerns identity theft. It provides that assuming a false identity of another person - living or dead, real or fictional, natural or corporate - makes a 'false pretence', even if the person acts with the consent of the person whose identity is falsely assumed.⁴³ The amendments also make it an offense for any person to falsely pretend to have possessed particular qualifications or capacities in order to acquire property, goods and services. The law likewise makes the following acts as an offense that would fall within its purview:

⁴³ <http://www.caslon.com.au/idcrimeguide16.htm> (last accessed December 30, 2009).

- a. using another person's personal identification information with the intention of committing, or helping to commit, a serious criminal offence;
- b. producing or possessing material that would enable someone to assume a false identity or to exercise a false right of ownership to a financial or non-financial benefit, with the intention of using it, or enabling another person to use it, for a criminal purpose;
- c. selling or giving material that would enable someone to assume a false identity, or to represent a false right of ownership to a financial or non-financial benefit, knowing that it is likely to be used for a criminal purpose; and
- d. possessing equipment for making material that would enable someone to assume a false identity, or to exercise a false right of ownership to a financial or non-financial benefit, intending to use it to commit one of the above offenses.⁴⁴

The Act also amended the Criminal Law Sentencing Act 1988 (SA) in order to help victims in re-establishing their identities. It has given victims the option to file an application in court for the issuance of a certificate that will attest to the fact that the personal identification information of the victim has been used by the identity thief. This remedy has made the rectification less burdensome.

Despite the fact that the Act has made specific provisions that may deal with identity theft, a cursory reading of its provisions will yield to the conclusion that being a criminal offense, it is still the police officers who exercise discretion as to whether or not a crime should be filed. In other words, victims have no right to take actions by themselves. Moreover, the criminal nature of the Act requires satisfactory proof of specific criminal intent to commit an offense before an identity thief may be held liable.

⁴⁴<http://www.austlii.edu.au/au/journals/PLPR/2004/8.html> (last accessed December 30, 2009).

IDENTITY THEFT IN THE DOMESTIC LEVEL

The inadequacy of Philippine laws to punish perpetrators of computer-related crimes and fraud has been exposed to the whole world when the government failed to prosecute the perpetrator, a student of AMA Computer College, of “I Love You” virus. It may be recalled that the said virus has caused billions of damage worldwide. Since then, a good number of bills were filed in the 12th, 13th and 14th Congresses to avert the occurrence of the same catastrophe and to address the problem of computer-related and cyber crimes and identity theft cases. It is thus worthwhile to revisit some of the good bills filed but unfortunately kept pending before the halls of Congress.

In 2001, House Bill No. 03241 or the “Anti-Cyber Crime Act of 2001” was filed with the objective of protecting and safeguarding the integrity of computers, computer systems, computer data and information from computer-related fraud, abuses and other fraudulent activities by providing penal sanctions against the perpetrators. The bill further seeks to create the Cyber-Crime Investigation and Coordinating Body that will primarily work on the deterrence of cyber crimes.

Aside from the “Anti-Cyber Crime Act of 2001”, bills concerning cyber-crimes were likewise filed in the year 2004. Among these were House Bills 02093 and 02237 known as “Cybercrime Prevention Act of 2004” and “The Philippine Center on Transnational Crime Act of 2004”, respectively. House Bill 02093 seeks to impose penalties for the following cybercrimes: a) illegal access to the whole or any part of a computer system or network; b) illegal interception; c) data interference; d) system interference; e) misuse of devices; f) computer forgery; g) computer fraud; and h) unsolicited commercial communication. While House Bill 02237 provides for the creation of Philippine Center on Transnational Crimes which is mandated to devise rules, regulations and programs for the prevention of transnational crimes such as, but not limited to, trafficking of persons, money laundering, cyber crimes, fraud and counterfeiting currency, terrorism, smuggling, piracy, illicit trafficking of narcotic drugs terrorism and fraud.

Certain bills that punish identity theft, phishing and misuse of identity by means of electronic messages were also filed in the Senate. Some of these are Senate Bills 2405, 1371, 1626, 1844 and 1885.

S.B. 2405⁴⁵ punishes any person who shall commit the act of phishing in the internet or instant messaging system with imprisonment of not less than two (2) years nor more than ten (10) years, or a fine of not less than fifty thousand pesos (Php 50,000.00) but not more than five hundred thousand pesos (Php 500,000.00) or both such imprisonment and fine, at the discretion of the court. S.B. 1626 likewise punishes phishing but provides a lower penalty of imprisonment for a minimum of six (6) months and one (1) day to a maximum of six (6) years and a fine of not more than Six Thousand Pesos (P6,000) but not less than Two Hundred Pesos (P200).

S.B. 1371⁴⁶ defines identity theft as fraud committed using the sensitive personal information of another individual with the intent to commit, or to aid or abet any unlawful activity that constitutes a violation of any existing laws and result in economic loss to that individual. It provides a penal sanction of imprisonment of not exceeding ten years or a fine ranging from one hundred thousand pesos (P100, 000.00) to five hundred thousand pesos (P500,000.00), or both at the discretion of the court. S.B. 1844, on one hand, seeks to protect the consumers and service providers from the misuse of computer facilities by others sending unsolicited commercial electronic mail over such facilities.

Senate Bill No. 1885⁴⁷, dealing with identity theft, defines it as a crime committed when an individual with fraud, malice, ill will, intent to malign or with perversion, uses another's relevant and sensitive personal information to

⁴⁵ An Act Further Protecting the Integrity of Electronic Transactions, Defining for the Purpose The Crime of Internet and Telecommunications Phishing, Providing Penalties Therefor and For Othe Purposes, Senate Bill 2406.

⁴⁶ An Act Prohibiting the Misappropriation of Personal Information in Database and Collections of Information, Providing a Mechanism for Protection Against Identity Theft, and for Other Purposes, Senate Bill 1371

⁴⁷ An Act Defining the Crime of Identity Theft, Providing Penalties Therefor and For Other Purposes, Senate Bill 1885.

take on that person's identity. The crime of identity theft covers:

- a. the misuse of one's personal identification cards including passports, social security, documents relating to tax matters and employment, credit cards and other dossiers that distinguishes a person from another;
- b. mail fraud;
- c. stolen personalities in the internet, chatrooms, text messaging system and other advanced technology gadgets or in the mechanisms or modes of information highway; and
- d. all other forms that tend to establish new identity to defraud the government or further a crime defined in existing laws.⁴⁸

Moreover, Section 2 of the bill provides that any violator shall be punished by imprisonment for not less than six (6) years but not more than twenty (20) years or a fine of not more than five hundred thousand (P500,000) pesos nor more than five million (P5,000,000) pesos or both imprisonment and fine at the discretion of the court. The bill likewise mandates the National Statistics Office (NSO) to work with the Department of Justice in assisting victims of identity theft and in correcting false or fraudulent entries.

In Committee Report No. 770, prepared by the Committees on Science and Technology, Constitutional Amendments, Revision of Codes and Laws and Justice and Human Rights and Finance, recommended the consolidation of Senate Bill Nos. 653, 1377, 1626, 1844, 2053, 2176, 2347, 2405, 2412, 2480, 3023, 3177, and 3213, taking into consideration proposed Senate Resolution Nos. 578, 915, 960 and 1263. These bills and resolutions were sponsored by Senators Angara, Escudero, Estrada, Legarda, Santiago, Villar, Roxas, Trillanes, Enrile, and Lapid. The consolidation paved way to Senate Bill No. 3553 or the "Cyber-crime Prevention Act of 2009".

⁴⁸ S.B. 1885, § 1.

S.B. 3553⁴⁹ is comprehensive in the sense that it covers any and all cyber-crimes offenses. It classifies these offenses into: a.) offenses against confidentiality, integrity and availability of computer data and systems; b.) computer-related offenses; and c.) content-related offenses. Illegal access, illegal interception and data interference are among the offenses that fall within the ambit of the first category. Computer forgery and computer fraud are punishable under the second category. Under the third category, on the other hand, the crimes being punished are cybersex and child pornography.⁵⁰ In

⁴⁹ An Act Defining Cybercrime, Providing For The Prevention, Investigation and Imposition of Penalties Therefor and For Other Purposes, Senate Bill 3553. As of the writing of this article. The bill was approved for Second Reading.

⁵⁰ SEC. 4. *Cybercrime Offenses.* -- The following acts constitute the offense of cyber-crime punishable under this Act:

A. Offenses against the confidentiality, integrity and availability of computer data and systems:

1. Illegal Access - The intentional access to the whole or any part of a computer system without right.
2. Illegal Interception - The intentional interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data: Provided, however, That it shall not be unlawful for an officer, employee, or agent of a service provider, whose facilities are used in the transmission of communications, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity that is necessary to the rendition of his service or to the protection of the rights or property of the service provider, except that the latter shall not utilize service observing or random monitoring except for mechanical or service control quality checks;
3. Data interference – the intentional or reckless alteration of computer data without right.
4. System Interference - the intentional or reckless hindering without right of the functioning of a computer system by inputting, transmitting, deleting or altering computer data or program.
5. Misuse of Devices -
 - a. The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:
 - i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or
 - ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act;

B. Computer-related Offenses:

1. Computer-related Forgery - (a) the intentional input, alteration, or deletion of any computer data without right resulting in authentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; (b) the act of knowingly using computer data which is the product

addition, the bill punishes aiding or abetting in the commission of cybercrimes and any attempt to do the same.

With regard to penalties, the bill provides a penal sanction of imprisonment of *prision mayor* or *prision correccional* or fine ranging from Two Hundred Thousand Pesos to One Million Pesos, or both fine and imprisonment, depending on the gravity of the offense committed.⁵¹

of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

2. Computer-related Fraud - the intentional and unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby, with the intent of procuring an economic benefit for oneself or for another person or for the perpetuation of a fraudulent or dishonest activity; Provided, that if no damage has yet been caused, the penalty imposable shall be one degree lower.

C. Content-related Offenses:

1. Cybersex - any person who establishes, maintains or controls, directly or indirectly, any operation for sexual activity or arousal with the aid of or through the use of a computer system, for a favor or consideration.

2. Child Pornography - any person who willfully engages in the following acts:

- a. Producing child pornography through a computer system;
 - b. Offering or making, available child pornography through a computer system;
 - c. Distributing or transmitting child pornography through a computer system;
 - d. Procuring child pornography through a computer system for oneself or for another person;
- or
- e. Possessing child pornography materials in the computer system or on a computer data storage medium.

For purposes of this Section, the term "child pornography" shall include pornographic material that visually depicts: (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; (c) realistic images representing a minor engaged in sexually explicit conduct.

⁵¹ SEC. 7. *Penalties.* -- Any person found guilty of any of the punishable acts enumerated in Sections 4,A and 4B of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two Hundred Thousand Pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both.

Any person found guilty of any of the punishable acts enumerated in Section 4C(I) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two Hundred Thousand Pesos (PhP200,000.00) but not exceeding One Million Pesos (PhP 1,000,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 4C(2) of this Act shall be punished with imprisonment of *prision correccional* or a fine of at least One Hundred Thousand Pesos (PhP100, 000.00) but not exceeding Five Hundred Thousand Pesos (PhP500,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 4C(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty Thousand Pesos

S.B. 3553 creates the Cybercrime Investigating and Coordinating Council (CICC) which has the functions and powers to: 1.) prepare and implement appropriate and effective measures to prevent and suppress cybercrime activities; 2.) monitor cybercrime cases being handled by participating law enforcement and prosecution agencies; 3.) facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution; 4.) coordinate the support and participation of the business sector, local government units, and non-government organizations in cybercrime prevention programs and other related projects; 5.) recommend the enactment of appropriate laws, issuances, measures and policies; 6.) call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions; and 7.) perform such other functions and duties necessary for the proper implementation of the Act.⁵²

Barely four (4) months before the closing of the 14th Congress, the bill is still pending for second reading. The author fears that the efforts of the men and women behind the bills consolidated will be rendered futile. The bill is in danger of not being passed into a law considering the fact that campaign and election period is fast approaching.⁵³

Nine (9) years after the "I LOVE YOU" virus incident, the Philippine legislature has failed to pass bills filed before it concerning cybercrimes and computer-related cases. Did it lose sight of the development in information and communications industry?

REPUBLIC ACT 8484

(PhP50,000.00) but not exceeding Two Hundred Fifty Thousand Pesos (PhP250,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one degree lower than that of the prescribed penalty for the offense or a fine of at least One Hundred Thousand Pesos (PhP100,000.00) but not exceeding Five Hundred Thousand Pesos (PhP500,000.00) or both.

⁵² S.B. 3553, § 22.

⁵³ Based on S. Ct. Res. No. 13, introduced by Senator Juan Miguel Zubiri, the Third Session of the 14th Congress will adjourn on February 6, 2010 until May 30, 2010. As of this writing, the said bill is still pending for Second Reading.

The State recognizes the use and importance of access devices⁵⁴ in commercial transactions. In order to regulate its use and to protect consumers from unauthorized and fraudulent use of the same, Congress enacted Republic Act 8484, otherwise known as "Access Devices Regulation Act of 1998". The law proscribes the conduct of counterfeiting and unauthorized use of access devices. It likewise prohibits the issuance of the same on account of use of falsified document, false information, fictitious identities and addresses, or any form of false pretense or misrepresentation. The specific acts considered fraudulent and unlawful were enumerated in Section 9 which provides:

"Section 9. Prohibited Acts. – The following acts shall constitute access device fraud and are hereby declared to be unlawful:

- (a) producing, using, trafficking in one or more counterfeit access devices;
- (b) trafficking in one or more unauthorized access devices or access devices fraudulently applied for;
- (c) using, with intent to defraud, an unauthorized access device;
- (d) using an access device fraudulently applied for;
- (e) possessing one or more counterfeit access devices or access devices fraudulently applied for;
- (f) producing, trafficking in, having control or custody of, or possessing device-making or altering equipment without being in the business or employment, which lawfully deals with the manufacture, issuance, or distribution of such equipment;
- (g) inducing, enticing, permitting or in any manner allowing another, for consideration or otherwise to produce, use, traffic in counterfeit access devices, unauthorized access devices or access devices fraudulently applied for;
- (h) multiple imprinting on more than one transaction record, sales slip or similar document, thereby making it appear that the device holder has entered into a transaction other than those which said device holder had lawfully contracted for, or submitting, without

⁵⁴R.A. 8484, § 3 (a) defines an access device as any card, plate, code, account number, electronic serial number, personal identification number, or other telecommunications service, equipment, or instrumental identifier, or other means of account access that can be used to obtain money, good, services, or any other thing of value or to initiate a transfer of funds other than a transfer originated solely by paper instrument.

being an affiliated merchant, an order to collect from the issuer of the access device, such extra sales slip through an affiliated merchant who connives therewith, or, under false pretenses of being an affiliated merchant, present for collection such sales slips, and similar documents;

(i) disclosing any information imprinted on the access device, such as, but not limited to, the account number or name or address of the device holder, without the latter's authority or permission;

(j) obtaining money or anything of value through the use of an access device, with intent to defraud or with intent to gain and fleeing thereafter;

(k) having in one's possession, without authority from the owner of the access device or the access device company, an access device, or any material, such as slips, carbon paper, or any other medium, on which the access device is written, printed, embossed, or otherwise indicated;

(l) writing or causing to be written on sales slips, approval numbers from the issuer of the access device of the fact of approval, where in fact no such approval was given, or where, if given, what is written is deliberately different from the approval actually given;

(m) making any alteration, without the access device holder's authority, of any amount or other information written on the sales slip;

(n) effecting transaction, with one or more access devices issued to another person or persons, to receive payment or any other thing of value;

(o) without the authorization of the issuer of the access device, soliciting a person for the purpose of:

1) offering an access device; or

2) selling information regarding or an application to obtain an access device; or

(p) without the authorization of the credit card system member or its agent, causing or arranging for another person to present to the member or its agent, for payment, one or more evidence or records of transactions made by credit card.

Any person found guilty of any of the acts mentioned in the above-cited provision shall suffer imprisonment for not less than six (6) years but not more than twenty (20) years and a fine of Ten Thousand Pesos (P10,000.00)

or twice the value obtained from the offense. The law further provides penal sanctions for the frustrated and attempted access device fraud. In case of the former, the perpetrator shall be punished with two-thirds of the fine and imprisonment imposed for the consummated offense while in case of attempted, the perpetrator is punished with one-half (1/2) of fine and imprisonment thereof.

One of the salient features of R.A. 8484 is that it creates a presumption or prima facie intent to defraud the mere possession, control or custody of:

- (a) an access device, without permission of the owner or without any lawful authority;
- (b) a counterfeit access device;
- (c) access device fraudulently applied for;
- (d) any device-making or altering equipment by any person whose business or employment does not lawfully deal with the manufacture, issuance, or distribution of access device;
- (e) an access device or medium on which an access device is written, not in the ordinary course of the possessor's trade or business; or
- (f) a genuine access device, not in the name of the possessor, or not in the ordinary course of the possessor's trade or business, shall be prima facie evidence that such device or equipment is intended to be used to defraud.

The law further provides that any cardholder who abandons or leaves the place of employment, business or residence stated in his application or credit card, without informing the credit card company of the place where he could actually be found, if at the time of such abandonment or surreptitious leaving, the outstanding and unpaid balance is past due for at least ninety (90) days and is more than Ten thousand pesos (P10,000.00), shall be prima facie presumed to have used his credit card with intent to defraud.⁵⁵

⁵⁵ R.A. 8484, § 12.

R.A. 8484 protects consumers from fraudulent activities such as identity theft and illegal use of credit cards through the regulation of the issuance and use of access devices. Through the stiff penalties it provides in case of violation thereof, it is aimed that fraudulent practices involving credit cards will be minimized, if not eliminated.

In the course of the implementation of the law, however, certain discrepancies were encountered by law enforcers and practitioners. These discrepancies and loopholes were caused by divergence in the application of the law.

In prosecuting Onel de Guzman, a student of AMA Computer College and the primary suspect in the spread of “I LOVE YOU” virus, the National Bureau of Investigation and the Department of Justice had conflicting opinions as to whether R.A. 8484 may be applied in the case.

The NBI contends that despite the fact that the virus was designed to shutdown computers by clogging the e-mail system, the virus also had a second purpose which is to fetch another program from a website in the Philippines that would sniff through the user’s computer for internet access passwords and e-mail those passwords back to an address here. NBI Officials were of the opinion that the virus was created simply to gather passwords in the Philippines. In effect, the author would be charged with using stolen passwords to connect to two Manila internet service providers, and not with actually unleashing the virus, which is not specifically prohibited by Philippine law. In support of their contention, they relied to Section 9 of R. A. 8484, which prohibits the act of disclosing any information imprinted on the access device, such as, but not limited to, the account number or name or address of the device holder, without the latter’s authority or permission; or obtaining money or anything of value through the use of an access device, with intent to defraud or with intent to gain and fleeing constitutes access device fraud. According to the NBI, with stolen user names and passwords, the author of the virus could have gained access to a multitude of computers, making this

law applicable.⁵⁶

The DOJ, nevertheless, in its opinion dated May 19, 2000, categorically stated that computer hacking is different from credit card fraud which makes the application of R.A. 8484 erroneous. This opinion was supported by Senator Ramon Magsaysay, Jr., as the primary sponsor of the e-commerce law, which said that the NBI was wrong to use the access device law because “they may be violating a citizen’s civil rights.”

Considering the above scenario, the author believes that R.A. 8484 failed to foresee a situation where access device fraud is committed by means of computers and digital equipments. In applying the said law, several questions do come in the picture. Is the enumeration provided in Section 9 of the law exclusive? What if the fraud was made through hacking or phishing, can the perpetrator be punished under R.A. 8484? Will there still be a violation of civil rights if R.A. 8484 is applied to cases of access device fraud by means of hacking or phishing? It is a known fact that fraudulent practices involving credit cards are presently committed by both individuals and syndicates. As development in technology progresses, the means employed by violators also progress. At times, technology has been the instrument of these perpetrators in consummating their evil motives.

The banking and credit industries face rising losses every year. This predicament has urged the CCAP to encourage Congress to focus on crafting laws that will curb credit card fraud. The group said amendments should be passed to upgrade the penalty clauses of the R.A. 8484 like treating large-scale credit card fraud as “economic sabotage”, with the accused perpetrators denied right of bail while litigation is pending in court.

A careful study of the law reveals its failure to address the problems of banking and credit industries. While it protects consumers, it however failed to protect these industries. It could have been more advantageous and beneficial

⁵⁶ Franklin I. Cueto, *A Study on Juan “spyder” de la Cruz’ case*, <http://ublawjournal.tripod.com/issue/jan-mar2000/astudyonjuan.html> (last accessed December 30, 2009).

if it provides remedies to both the consumers and banking and the credit industries.

E-COMMERCE ACT, A LANDMARK LEGISLATION

Six weeks after the “I LOVE YOU” virus attack, the government has outlawed some computer crimes through the E-Commerce Law. The Electronic Commerce Act of 2000 or Republic Act 8792 was signed into law on June 14, 2000. It was a landmark legislation as it was the country’s response to the changes brought about by the information age. It focuses more on electronic evidence and common online crimes such as hacking and copyright violations.⁵⁷

The Philippine Congress enacted R.A. 8792 in order to provide a legal framework for internet-based services such as electronic commerce. It has given an electronic document and electronic signature⁵⁸ legal binding effect same as that of a paper-based document. Aside from the provisions on e-commerce, the law also seeks to punish perpetrators of cybercrimes particularly computer hacking, introduction of viruses and piracy of copyrighted works by providing penal sanction thereof. Thus, Section 33 of the law provides:

“SEC. 33. Penalties. - The following Acts shall be penalized by fine and/or imprisonment, as follows:

(a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without

⁵⁷ Joel D. Pinaroc, *Philippines Mulls Over Cybercrime Laws*, <http://www.zdnetasia.com/news/business/0,39044229,62034883,00.htm>, (last accessed November 14, 2009).

⁵⁸ R.A. 8792, §5 (e) defines electronic signature any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document. An electronic document, as provided in Section 5 (f), refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

(b) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

x x x

As can be gleaned from the above-cited provision, R.A. 8792 focuses only on common on-line crimes. It failed to include the more nefarious crimes such as child pornography, phishing and identity theft. A careful study of the law would lead to the conclusion that the law made mention of the crimes of hacking and piracy only in Section 33. No specific provision has been provided to define the scope and coverage of crimes of hacking, introduction of viruses and piracy. Moreover, most, if not all, of the provisions are in line with the objective⁵⁹ of the Act which pertains to the protection and promotion of

⁵⁹ R.A. 8792, § 3. *Objective.* - This Act aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information through the utilization of electronic, optical and similar medium, mode, instrumentality and technology to recognize the authenticity and reliability of electronic documents related to such activities and to promote the universal use of electronic transaction in the government and general public.

dealings, transactions, contracts and arrangements by electronic means.

It can also be gleaned from the provisions of R.A. 8792 that it likewise deals on the admissibility of electronic documents and electronic signatures as evidence. Some provisions set the guidelines or rules pertaining to the introduction of the same.

REGULATORY MEASURE OF THE EXECUTIVE DEPARTMENT

On April 13, 2005, President Gloria Macapagal Arroyo, in the exercise of her residual powers⁶⁰, issued Executive Order No. 420⁶¹ or the Unified Multipurpose ID (UMID) System which mandated the National Economic and Development Authority (NEDA) to implement the same.⁶² E.O. 420 is a means of streamlining government services and processes by unifying all existent government-issued ID cards into one card that can be used for all

⁶⁰ The exercise by the President of residual power is founded on his duty as steward of the people. It is a power borne by the President's duty to preserve and defend the Constitution. It also may be viewed as a power implicit in the President's duty to take care that the laws are faithfully executed. (*Marcos v. Manglapus*, 177 SCRA 668 (1989) at 694) The residual power of the President is likewise provided in Chapter 7, § 20 of the Administrative Code of 1987 which provides:

“Sec. 20. Residual Powers. - Unless Congress provides otherwise, the President shall exercise such other powers and functions vested in the President which are provided for under the laws and which are not specifically enumerated above, or which are not delegated by the President in accordance with law. “

⁶¹ In *Kilusang Mayo Uno, et al. v. Director-General of the National Economic Development Authority, et al.*, 487 SCRA 623 (2006), the Supreme Court upheld the constitutionality of E.O. 420. It held that the same does not establish a National Identification System. The Congress still exercises the power and/or authority to enact a law establishing the National ID System. The said law falls within the power of the executive to enact laws for effective and efficient enforcement of existing laws.

⁶² E.O. 420 § 4, provides: *Authorizing the Director-General, National Economic and Development Authority, to Harmonize All Government Identification Systems.* – The Director-General, National Economic Development Authority, is hereby authorized to streamline and harmonize all government ID systems.

In addition to the powers of the Director-General, he is authorized to call on any agency or department of government, or to create committees and sub-committees for the effective and efficient implementation.

government transactions.⁶³ Among the objectives of the said law is to enhance the integrity and reliability of government identification cards⁶⁴ in order to minimize, if not, eliminate fraudulent transactions arising from identity theft or use of fictitious or false identities.

Section 6 of E.O. 420 provides that data to be collected and recorded shall be limited to the following: a.) name; b.) home address; c.) sex; d.) picture; e.) signature; f.) date of birth; g.) place of birth; h.) marital status; i.) name of parents; j.) height; k.) weight; l.) prints of index fingers and thumbmarks; m.) description of any prominent distinguishing features like moles and others; and n.) Tax Identification Number (TIN). These information shall be treated with strict confidentiality that only the owner of the data can authorize the access of the same. Further, the law has limited application as it covers only members or constituents of SSS, GSIS, DFA, POEA, Philippine Postal Office and BIR.

Despite the fact that the law aims to enhance the integrity and reliability of government IDs, the UMID card, however, serves only as a “convenience card” for the holder thereof can easily access and avail services and directly transact business with banks by sole reliance to the card. There is no 100%

⁶³ http://www.neda.gov.ph/ads/press_releases/pr.asp?ID=795 (last accessed January 2, 2010).

⁶⁴ Section 1. *Adoption of a unified multi-purpose identification (ID) system for government.* – All government agencies, including government-owned and controlled corporations, are hereby directed to adopt a unified multi-purpose ID system to ensure the attainment of the following objectives:

- a. To reduce costs and thereby lessen the financial burden on both the government and the public brought about by the use of multiple ID cards and the maintenance of redundant database containing the same or related information;
- b. To ensure greater convenience for those transacting business with the government and those availing of government services;
- c. To facilitate private businesses and promote the wider use of the unified ID card as provided under this executive order;
- d. To enhance the integrity and reliability of government-issued ID cards; and
- e. To facilitate access to and delivery of quality and effective government service.

guarantee that transactions will be fraud-free.

While it is true that UMID can be a means to enhance the integrity of government IDs, this measure, however, is not sufficient to combat the rising number of identity theft or identity fraud. Cases of identity fraud involving passports, birth certificates, SSS and GSIS membership cards continue to increase every year. While there is no doubt that government issued cards provide greater convenience to members or constituents, doubts, nonetheless, still exist as to its integrity and reliability.

ANALYSIS AND CONCLUSION

Hardly do Filipinos hear and read the words identity theft or identity fraud. These terms and issues may seem unfamiliar but that does not follow that the Philippines has been excused from experiencing its horrifying effects. It is actually one of the problems hounding the government. It is a problem that chooses no one. Young or old, rich or poor, powerful or powerless is not immune from the effects of identity theft. In other words, everyone can be a victim.

To illustrate, a local administrator in Bulacan has been victimized when someone used her e-mail account to send messages to her family, friends and colleagues, saying that she badly needed money because she was stranded in West Africa. Her friends received on June 27, 2007, an email with the subject “Please, I need your help.”⁶⁵

The e-mail said the administrator said she was attending a conference in West Africa when she lost her wallet, ATM card, passport and other valuables. The person who was using the identity and sensitive information of the administrator asked the latter’s contacts to send the money through a money gram so she could pay for hotel accommodation. The administrator said she learned about the hoax when she received several calls from her contacts in the Philippines and abroad asking about her whereabouts and to verify if she

⁶⁵ Philippine Daily Inquirer, “*Bulacan Official Falls Victim to Identity Theft*”, July 8, 2007

indeed needed financial help. Shocked, the administrator's host personality clearly stolen, tried to open her e-mail account but she was permanently barred from accessing her ID number and password.⁶⁶

In another incident, a woman applying for passport was surprised when her application was denied on the ground that records showed that another person already owns the identity. These two (2) cases were just among the several harrowing cases of identity theft.⁶⁷

Identity theft is committed in various ways. It is too unfortunate that most of the time, technology has been a tool to perpetrate this crime. E-mails, social network sites, digital equipments, computer and internet are just some of the means employed to steal personal identification and information which are used to derive financial benefits. With the rising number of Filipinos who avail the services of internet, SNS, e-mail and computer, identity theft cases also increase in number.

ID Theft affects both victims and banking and financial institutions. It cannot be denied that it causes great financial losses to individuals and institutions. Aside from this, what is more alarming is the intrusion of identity thieves into the right to privacy of every individual. The personal identity and information of an individual is part and parcel of his privacy. Thus, no one is allowed to intrude to this sacred right.

Philippines, being a signatory, in the United Nations Convention on Human Rights, has signified its commitment to its mandate that that "no one shall be subjected to arbitrary interference with his privacy" and "everyone has the right to the protection of the law against such interferences or attacks"⁶⁸. The question now is: Has the government taken concrete actions to protect

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ UN Convention on Human Rights, Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

its citizens from arbitrary interference with their privacy? Identity theft is an illegal, unlawful and arbitrary intrusion to the right of privacy. Has the legislature passed any law that will deter, counter and punish such intrusion?

The fundamental law of the land has given Congress the power to enact, amend and repeal laws. It has likewise been vested with the authority to conduct investigations in aid of legislation. The latter power has been always used by Congress to justify any and all investigations that it undertakes, even if at times it only involves trivial issues. It is too unfortunate that these trivial issues are given more attention by Congress that every so often, it fails to recognize the more important issues that need to be addressed.

Congress should be a venue for more critical debates on matters of great concern. It should not lose sight of matters that may jeopardize or threaten some of the valued rights of the people. It must discern on the problems posed by the modern world.

The author is of the opinion that Congress, up to this moment, has failed to recognize the impending effects of identity theft on the people, financial institutions and government agencies. The inaction of the legislature may possibly be attributed to the belief that existing laws are already sufficient to combat the problem. This however, is not the case. The legislative and regulatory responses of the government are not adequate to lessen, if not eliminate, the growing problems of identity theft.

Credit card fraud is just one aspect of identity theft. It is just but one of the means used by identity thieves to gain economic benefit. The author believes that the decade long application of R.A. 8484 should invite the attention of the lawmakers of the need to make certain amendments thereto in order to cope with the advancement in technology. Law-makers should consider the fact that these improvements provide greater resources to perpetrators to carry-out their ill motives. The amendments should provide a broader and wider enumeration of punishable offenses so as to include credit card fraud by means of hacking and phishing.

Moreover, it is not enough to punish ID Theft committed by means of internet and computer. The author believes that it is not correct to consider ID Theft as a mere cyber-crime. Internet and computers are just among the several means used to consummate identity theft. To consider it as one is like closing one's eye to the real nature of identity theft.

The problem of identity theft does not only require a positive action on the part of Congress. It also entails certain responsibilities to the executive branch. Regulatory measures should be undertaken in order to ensure the safety, confidentiality and credibility of sensitive data or information before the various agencies of the government. The government may consider the following recommendations of the author in the regulation of identity theft:

- a. Designate a coordinating body that will closely monitor and work identity theft complaints. This body shall likewise work hand in hand with government agencies and financial institutions in thwarting ID Theft;
- b. Formulate policies on the storage and safe-keeping of personal information of individuals and electronic shredding of the same in order to guarantee confidentiality and integrity. These policies shall be reviewed periodically in order to determine necessity of updating the same; and
- c. Formulate policies concerning internal staffs handling sensitive data or information to ensure that data are not improperly disclosed.

The international community has started taking actions to counter identity theft, and it is nonetheless too sad that the Philippine government has lagged behind. While the men and women behind the bills punishing identity theft, cybercrime offenses and computer-related offenses may be commended for their efforts to provide Filipinos timely and more beneficial laws, they still carry the challenge of working harder to make such bills pass into law.

As long as the legislature remains contented with the laws that this country already have, identity theft will continue to proliferate. Passing an identity theft law is the initial step to bring identity thieves within the reach of law enforcement agencies and officials.

The Philippines has been cited to be the social networking capital of the world. If the government continues with its inaction in combating the widespread identity theft, it will not be surprising if the Philippines becomes the identity thieves capital of the world. It will be easy for this country to be the haven of identity theft criminals. It is up to the government whether to allow this country to experience such fate.

It is always said that experience is the best teacher. One's level of maturity and efficiency is sometimes measured by his capacity not to commit the same mistakes he has committed. The author hopes that the government be reminded of the lessons left by the 2000 "I LOVE YOU" virus catastrophe. This is the opportune time for real actions.