附錄 3: 防制「身份竊取」立法策略之比較與分析
An Analysis and Comparison of Government Legislative Strategies for Preventing Identity Theft

I. Introduction

1. Background: Identities in the information society

An "Information society", which consists of computers, the Internet and flowing "information", is a formal and suitable name to describe our contemporary world. In this society, traditional "fact to face" activities have been replaced by communication and transactions via the Internet, that is to say, a receiver of an message has no real idea of who the sender is[1]. On this basis, identity, which can be used to distinguish an individual, is very essential to the Internet world; in other words, identity is very valuable. In addition, today, most information, even not all, is digitalized and unfortunately, digitalized items are very easy to duplicated, disseminated, more importantly, without any consciousness.

All these characteristics contribute to the serious identity theft problem in our modern world. To deal with the identity theft, the government, individuals and organizations that process and hold others' identities all may have their roles. Nevertheless, the government is the most significant one, at least in terms of legal aspects, because the government has power to mandate laws and enforce laws. From this standpoint, effective and comprehensive legislations are the foundation stones of identity theft prevention. To illustrate what kinds of legislations can be used to defeat identity theft, in the beginning, this article will discuss the definition and scope of identity theft, then discussing the process of an identity theft and how many roles involved in it. After that, an economic model will be introduced to analyze the effectiveness of every possible kind of legislations and, therefore, indicate some practical ones. In the middle part of this article, three different kinds of legislations will be mentioned, including UK and US related laws. After introducing the basic ideas and rules of individual legislations, some drawbacks of them will be illustrated as well. In the final part, the comparison is made and some suggestions, with regard to identity theft prevention in Taiwan, are proposed based on the foregoing discussions and comparisons.

2. What is identity theft—the definition

The definition of identity theft varies in different countries and different fields.

[1] Reed, C.: Internet Law: Text and Materials. Cambridge Press, Cambridge (2004), P140.

Generally speaking, the definition of identity theft falls into two major distinctive categories:

(1) 'Identity theft' is defined by the Oxford English dictionary as comprising the dishonest acquisition of personal information in order to perpetrate fraud, typically by obtaining credit, loans, etc., in someone else's name[2]. That is to say, when people's identities are unlawfully acquired by others[3], with intent to commit a crime, not just a fraud[4], an identity theft is committed.

(2) On the other hand, someone may argue that the appropriation of an identity of itself will not give rise to a criminal offence; using identities to commit frauds or other offences is identity theft. Moreover, to speak more specifically, "identity theft means a fraud committed or attempted using the identifying information of another person without authority"[5]. Therefore, based on this limit and argument, identity theft equals identity fraud[6].

From legal aspects, the different term 'theft' and 'fraud' are quite different terms, therefore, "identity theft" and "identity fraud" should be two distinct but close concepts. In terms of 'fraud', identity theft happens when personal confidential information is obtained by someone else without owner's explicit consent. On the other hand, identity fraud occurs when defrauders use the illegally-obtained personal information for financial gain. In this article, the former definition of 'identity theft' will be adopted; thus a further explanation will be render in some special circumstances.

3. Offences in relation to identity theft

(1) Fraud

The most common and harmful, in respect of financial loss, offence in relation to identity theft is definitely fraud. According to an USA Federal Trade Commission (FTC) Survey Report[7], an identity theft may be involved fraudulent uses in three major ways: appropriate of victim's credit card, the opening of a new credit in victim's name and the opening of a bank account and the running-up of an overdraft or the

---

[2] Oxford English Dictionary, http://dictionary.oed.com Accessed 1 Aug 2008

[3] Walden, I.: Computer Crime and Digital Investigations, Oxford University Press, Oxford (2007), P115

[4] 18 U.S.C. § 1028(a)(7)

[5] 16 C.F.R. § 603.2 (a)

[6] Mercuri, R. T.: Scoping identity theft, Communication of the ACM 49(5) P17-21 (2006)

[7] Synovate: 2006 Identity Theft Survey Report. http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (2007) Accessed 1 Aug 2008

taking-out or other loans with personal details[8]. By having this information, a thief can even change the billing address for the account so that the unauthorized purchase or loans remain uncovered[9].

In Taiwan, defrauders may use the individuals' identities to commit fraudulences in slightly different ways. There are two common ways in respect of the instruments they use: the first one is that the defrauders phone the victims directly. In that phone call, the defrauders purport that he is from some kinds of authorities and, via knowledge of victim's confidential personal information, make victim trust him. Then the defrauders play to alert the victims to that some fraudulent activities on their credit cards or bank accounts and, the accounts involved would be froozen by legal authorities in order to minimize the loss incurred. Due to panic and anxiety, the victims always have no choice to follow the defrauders' instrutions to use cash machines to transfer money from the victim's account to another account, an 'dummy account' which is opend with stolen identities or is offerd by third parites. The money transferred into the 'dummy account' is always, not surprisingly, withdrawed by the defrauders or other conspirators immediately. In the second way, defrauders harness mail system rather than phone. The defrauders delivery spoofed offical documents, such as banking letters, supernos or confiscation orders, containing specific personal identitites to deceive the victims that they would be on the aim of subsequent legal actions against them. These forge documents are often with 'advices' which recommend the victims to dail a telephone number on the documents to get more detail infotmaion. When victims call this number, the defrauders, as in the first way, pursuad the victims to tranfer the money from his 'alleged endangered account' into the 'dummy account' controlled by the defrauders. To sum up, unlawfully obtained identities are involved in the special frauds in Taiwan in two ways: the first is that the defauders use the identities to make the victims trust them and, the second is that the defauders may use the identities to open an 'dummy account' and use these accounts to commit fraudlences. In both ways, stolen identitites are essential and fundemental tools to commit frauds.

(2) Money laundering

Identity thieves get involved in the money laundering in two respects: the first one is that in order to prevent the use of the financial system for the purposes of money laundering, money laundering regulations in many countries have been made to order

[8] ibid. P3

[9] Elbirt, A.J.: Who are you? How to protect against identity theft. IEEE Technology and Society Magazine, Summer P5-9 (2005)

persons carrying on relevant transactions must comply with requirements relating to identification procedures[10]. For example, US law has required finanical instiutaion to file currency transaction reports for large currency transaction and verify the indiviual's identity; the present reporting threshold applies to currency trancsaction in excess of $10,000[11]. As a result, a money launder who desires to keep his real indentiy secret to avoid tracing needs false identiy. The second respect is that money launder may need some 'dummy accounts', accounts created with stolen identities, to transfer money and conceal the source and identity of money.

(3) Other offences

Besides the above offences, various offences also appear as long as the victims' identities lost. For example, the defendant may submit others names and driving license numbers during the arrest[12]. Terrorists, on the other hand, may use stolen identities to conceal their real identities or the original sources of money[13].

4. What kind of information constitutes an identity

The term "identity" is often used in an arbitrary and imprecise manner in popular media and literature[14]. In general, identity of a person is defined as 'the qualities of a person or group which make them different from others'[15]. But the term 'identity' in the 'identity theft' should embrace other features. At first, in general, the 'identity' here is easily copied or stolen, in other words, reproduction of identity cost little. On this ground, fingerprints and other 'biological identities' should not be included under this definition. However, financial information such as bank statements and purchasing records, or personal information such as address and occupations, which can not be used to distinguish an individual but still could be targets of identity theft.

Based on the foregoing features, the 'identity' can be generally categorized as two classes: the first one is the traditional identity which can be used to make one person distinguished from others and should be easily stored, copied and transferred, such as social security numbers, birth of dates, even criminal records etc. The second class is

---

[10] Such as the UK Money Laundering Regulations 2003, SI 2003/3075, Reg. 4.

[11] 31 C.F.R. §103.30

[12] Marron, D. :Governing the Risk of Identity Theft. British Journal of Criminology 48(1) P20-38 (2008)

[13] Linn, C.J.: How terrorist exploit gaps in US anti-money laundering laws to secrete plunder. Journal of Money Laundering Control 200 8(3) 200-214 (2005)

[14] Chawki, M., Abdel, M.S.,: Identity Theft in Cyberspace: Issues and Solutions. Lex Electronica 11 (1) (2006) http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.htm. Accessed 26 June 2008

[15] Cambridge Dictionaries Online, http://www.dictionary.cambridge.org. Accessed 26 June 2008

valuable information which can not be used as an identity alone, but can be used to help the identities of the first class to prove to be genuine or, help to describe the characteristics of an individual. For example, a bank statement alone, in the UK, can not be used as an identity, but may be used as an auxiliary to assist other identities when applying for a permission of a public library. Among all identities above, the social security numbers in the US, or identity card or identity numbers in other countries, may give rise deep concerns. The common feature of this kind of identity is that it surpasses all other identities under most circumstances; in other words, it may be considered as the 'master key' in all situations in need of identities[16]. The common reliance on this kind of identify creates an easy and appealing target for identity predators[17]. This 'dominating' characteristic arise some doubts and that is the main reason of the opponents of the UK national ID Programs[18], who regard the ID number as being too easily to be copied and too vulnerable as a result.

5. How serious identity theft is

(1) The UK

By virtue of that financial loss due to identity theft is more easily to estimate, in the UK, all main reports are in relation to the identity fraud, rather than the loss of identity theft as a whole. The 2002 Cabinet Office Study, which covered the use of false identities and the theft of other people's identities, estimated that crime facilitated by identity fraud cost the UK £1.3 billion per year[19]. Recently, the Home Office Identity Fraud Steering Committee updated and the latest estimate is that identity fraud costs the UK economy £1.7 billion[20]. This figure is an increase of 400 million on 2003 estimates and indicates that this is a problem on the rise[21]. However, although this figure includes the damages of fraudulent and the prevention costs, it does not include the cost of the victims spend on recovering their lost identities and the mental threat of the victims. Separately, in January 2008, the Information Commissioners Office (ICO) launched its new research relating to the awareness of identity fraud. In stead of the

---

[16] ibid. 9

[17] Valetk, H. A.: Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies. Stanford Technology Law Review 2 (2004)

[18] LSE: Identity Project Report. Chap.8 http://is2.lse.ac.uk/idcard/identityreport.pdf. Accessed 6 Aug. 2008

[19] Metropolitan police service: Fraud Alert - Identity Theft/Fraud. http://www.met.police.uk/fraudalert/section/identity_fraud.htm. Accessed 2 Aug. 2008

[20] Home Office Identity Fraud Steering Committee: Updated Estimate of the Cost of Identity Fraud to the UK Economy. http://www.identity-theft.org.uk/ID%20fraud%20table.pdf. Accessed 2 Aug. 2008

[21] All Party Group: All Party Parliamentary Group Report to Identity Fraud. http://www.fhcreative.co.uk/idfraud/downloads/APPG_Identity_Fraud_Report.pdf. (2007) Accessed 2 Aug. 2008

economic loss, this research showed how rampant identity theft is in another way: 1 in 5 people believe that they have been a victim of identity crime; young people between 16 and 25 are most vulnerable as they are the least protective of their personal information[22].

(2) The US

A FTC report showed that, in the US, a total of 3.7 percent of survey participants indicated that they had discovered, rather than believed as we have seen in the UK report, that they were victims of identity theft in 2005; accordingly, almost 8.3 million U.S. adults discovered that they were victims of some form of identity theft in 2005[23]. With regard to the loss caused by the identity thieves, the report showed the figures in two aspects: one is the financial value obtained by the thieves and another is the cost spent by the victims. The median value of goods and services obtained by identity thieves for was $500, that is to say, the expected total value for the U.S. adults was $4.15 billion. In respect of the cost spent by the victims, two parts of cost should be concerned: the expenses and time. According to the report, although 50 percent of the victims incur no expense, the average expense incurred by the victims was $ 40 and average hours spent by the victims to resolve their identity problems was 10 hours.

(3) Taiwan

The statistics with regard to identity theft, including the number of identity thieves, victims or figures of financial losses, has not been available yet. However, the statistics in relation to other offences may have provided us a vague but illustrating image about the severity of identity thefts in Taiwan. As we have seen above, several kinds of frauds, such as phone or mail frauds by false representations are committed by using victims' stolen identities. The police statistics report showed that from 1st January 2008 to 31st May 2008, the total number of frauds in relation to false representation is approximately 14,000[24] during those five months.

II. The roles involved in and the whole process of identity theft

1. How to steal the identities

The common ways of how the identity thief get victim's are as follows:

---

[22] ibid

[23] Ibid 7

[24] National Police Agency: Police Statistic Report. http://www.npa.gov.tw/NPAGip/wSite/public/Attachment/f1214883575167.doc. Accessed 6 July 2008

(1) Stolen wallets, credit cards and checkbooks[25]

Stolen wallets and purses, with persona identity cards, credit cards or address books, definitely constitute a good source of personal identities.

(2) By known people

According to FTC 2006 Survey Report, 16% percents of all identity theft victims claimed that their personal information was taken by someone they personally knew, including family members, relatives and in-house employees[26].

(3) Garbage diving

The discarded bank account statements, credit card statements, or garbage is a good resource of personal identities, where credit card numbers, date of birth and others personal confidential information may be leaked.

(4) Unlawfully obtained from legal resources:

One of the major sources of identities is unlawfully obtaining personal identities from legal databases. For example, a former or incumbent policeman may access to contents in the police database then divulged it[27] and city council register may sell information of new born to health institutions. .

(5) Phshing

The word "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the Internet users[28]. In general, phishing attacks harness the technology of the Internet and software to create fraudulent emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. In other words, phishing is an online activity that combines social engineering strategies and technical measures[29]. The number of unique phishing websites detected by the

---

[25] The Javelin Strategy and Research: 2008 Identity Fraud Survey Report. http://www.idsafety.net/803.R_2008%20Identity%20Fraud%20Survey%20Report_Consumer%20Version.pdf. (2008) Accessed 6 Aug. 2008

[26] ibid 7. P30

[27] Information Commissioner's Office: ICO Report: What price privacy now? http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico-wppnow-0602.pdf. (2006) P15 Accessed 6 Aug. 2008

[28] Anti-Phishing Working Group: Origins of the Word "Phishing" . http://www.antiphishing.org/word_phish.html. Accessed 6 Aug. 2008

[29] Anti-Phishing Working Group: What is Phishing and Pharming? http://www.antiphishing.org/.

Anti-Phishing Working Group (APWG) in May 2007 was 25,328[30].

For example, in the following example, figure 1, a victim receives a phishing email purporting to come from a trustworthy party, Woodgrove Bank. This email has a link to a counterfeit website. The email and the creation of the website are designed to trick the victims to believe that Woodgrove Bank has been the initiator of the communication. As long as logging in this fake website, the victims soon leak all confidential information, such as passwords, birth of date and social security number to identity thieves.

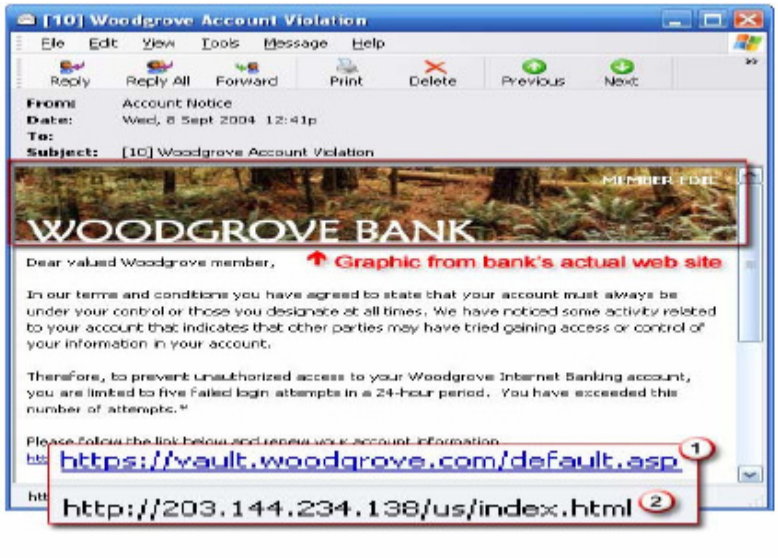

Figure1 A phishing mail sample[31]

(6) Vishing

Vishing is a traditional offence but using quite new technology and, from the perspectives of victims, it is very similar to phishing but with a few of variations[32]. Vishing exploits the victim's trust in landline telephone services rather than by email. Using the new technology VoIP (Voice over Internet Protocol)[33], vishing can take several advantages, comparing to the traditional wire frauds or phishing[34]. At First, VoIP service is quite inexpensive, especially for long distance, making it cheap to make fake calls. Secondly, because it's web-based, criminals can use software

---

Accessed 6 Aug. 2008

[30] Anti-Phishing Working Group: Phishing Attack Trends Report - December 2007, http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf Accessed 6 Aug. 2008

[31] http://www.microsoft.com/protect/yourself/phishing/identify.mspx Accessed 6 Aug. 2008

[32] FBI: Something Vishy-Be Aware of New Online Scam. http://www.fbi.gov/page2/feb07/vishing022307.htm. Accessed 6 Aug. 2008

[33] Wikipedia: Voice over Internet Protocol. http://en.wikipedia.org/wiki/Voip. (2008) Accessed 10 Aug. 2008

[34] ibid.

programs to create phony automated customer service lines[35], and the victim is often unaware that VoIP allows for caller identity spoofing.

(7) Spyware

A spyware can be loosely defined as "'deceptive' practices of the unauthorized installation of programs that monitor a consumer's activities without their consent."[36]. The installed spyware can then be used to send the user unwelcome pop-up advertisement, take control of the users' web browser, monitor the users' Internet surfing habits, record the users' keystrokes and even steal personal confidential information stored in the computer[37]. A report alleged that since 2004 this method of obtaining confidential information, which involves the victim clicking on an innocent looking email from a defrauder, has risen by 250%[38].

(8) Mail fraud or wire fraud

In addtion to phishing or vishing, other kinds, or traditional kinds we may say, of false representation also appear. A number of schemes which misrepresent the identity of the sender, delivering forged documents for personal information have also been perpetrated by mail; forged taxation document requisting banking information is the most common form[39].

In the above eight ways, the first three ways are fairly common but relatively in small scale, in other words, most identities lost in these three ways only involve one or two persons. However, the identities lost in the rest often involve a lot of people. On this ground, the methods to prevent identitis lost in the ways of these two different classes should be different. The thievies stealing identites in ways in relation to a massive extent should be tackled differently, more like to deal with as oganized crimes and worth special treatments. On the other hand, the first three ways involving fewer people are comparatively uncomplicated and, accordingly, special strategies are not necessary. .

2. How to use stolen identities to commit crimes

---

[35] ibid.

[36] Rasch, M.: Is Deleting Spyware a Crime?. Spyfocus. http://www.securityfocus.com/columnists/328. (2005) Accessed 6 Aug. 2008

[37] FTC: FTC Consumer Alert: Spyware. http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.pdf. (2004) Accessed 6 Aug. 2008

[38] Hamilton-James, L.: identity theft. 27 Link AWS. p8-9. (2007)

[39] Wikipedia: Mail Fraud. http://en.wikipedia.org/wiki/Mail_fraud. Accessed 6 Aug. 2008

As we have seen above, in general, the identity theft itself is a precursor of fraudulent and other offences[40]. From this perspective, we may divide the whole process from when individuals lost their personal identities to final sufferings due to related offences into three main stages, as shown in the following diagram:

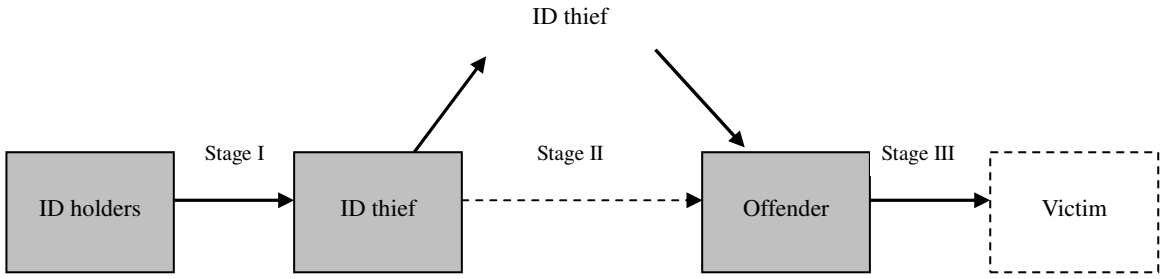

Figure 2: The three stages of identity theft and roles involved

There are three stages appearing the above figure: the identity theft, unlawful trade and committing crimes. The first stage, the process is clear: individuals lost their identities, no matter by phishing, spyware or other ways.

In the second stage, identity traders who sell the personal information obtained from others or by themselves are also very important roles involved in the identity theft[41]. They, even they just sell the information obtained from others, not directly obtaining identities from individuals or corporations holding information, but still have great influence on the whole process in two respects. At First, the thieves who steal the identities may not have direct channel to connect to offenders who really use the identities to commit crimes. The traders, as an agent under this circumstance, narrow the gap between the other two parts. Secondly, in general, a thief may only steal one or more kinds of identities which available to him, but not enough to commit crimes. For example, a bank clerk can only steal information in relation to an bank account which includes as more as names, account numbers etc; other valuable information, such as crime records, drive license numbers, family names of the account holder are not accessible. In other words, offenders have to access to more than one sources to

[40] ibid 3, P161.
[41] ibid 27, P15

obtain all identities they need. At this time, a trader who can collect various identities from different sources can give offenders great assistance in terms of lower cost, and most importantly, a set of complete identities which they need for committing specific crimes.

The last stage is that offenders use stolen identities to commit the crime, such as opening credit accounts, forging a license etc. In this final stage, the individuals, the lawful identity holders, will suffer the damage from the identity theft.

According to the three stages above, we can find out that five roles may be involved in the whole course of identity theft: identity holders, identity thieves, identity traders, offenders and victims. The "identity holders' are individuals, originations and institutions that have confidential identities. The identities possessed by an identity holder may be belonged to himself or, sometimes, to others. For example, a bank often possesses a great deal of customer's information and a register in a school may hold the identities of him as long as confidential information of all students. The second role, an "identity thieves", is the one who steals or unlawfully gets identities from identities holders. The "traders", rather than stealing identities by themselves, trade the identities and obtain benefits from the trades. The "offenders" are the criminals who use stolen identities to commit offences, such as frauds and other offences. The last role, the victim, suffers the offence; for example, the bank in the bank fraud in connection with stolen identities. Nevertheless, these five roles may not all appear simultaneously: some roles are played by the same character in some cases; for instance an identity thief who steals identities may himself or herself use the identity to commit fraud. Furthermore, the stolen identities may be used for lawful purposes, such as marketing or researches; as a result, the offenders and the victims of the following offences are missing under this circumstance. On the same ground, a trader is not a necessary part since some identities may trade the stolen identities directly without any agency or inter-mediator. Briefly speaking, the first two roles, the identity holders and identity thieves, are both essential in the whole course of identity theft and, the rest three of them are optional. We use different lines to tell them apart in the diagram.

3. Who can prevent identity theft

After discussing the whole process of and the five roles involved in the identity theft, with regard to identity theft prevention, the next thing we have to analysis is who can or, who has the power to prevent identity theft.

(1) Individuals and identity holders:

The individuals, or more generally speaking, identity holders may play a most direct and important role in identity theft prevention. The reason of this argumentation is very simple: the man who obtains the objects can easily take measures to defend the objects and has the strongest incentive to do those. Accordingly, there is much assistance available to identity holders in identity theft prevention. For example, individuals are suggested to regularly check their identities to avoid loss caused by identity theft[42]. On the other hand, professional identity holders, such as banks may be advised to take some technical measures to avoid hackers[43].

(2) Victims of Offences

Similar to identity holders, victims of offences are a group of people have strongest incentives and greatest opportunities against identity theft. That is why it is more common to see that ordinary people have been educated in protecting themselves against frauds, tracing fraudulent activities so that it can be disrupted at an earlier stage and bring cases much more quickly to court.

(3) Government

Instead of the identity holders, the government, on the other hand, play a gradually important role in identity theft prevention. The most obvious reason is that government, rather than the individuals or organizations, is mandated powers to launch rules, like crime codes, and create institutions, like professional detectives, against identity theft. Additionally, identity theft ,which has been suggested in some recent cases, are progressively evolving from personal tricks to organized crimes; on this ground, government is the only one who have plenty of resources and can coordinate, organize and regulate separate and accordingly vulnerable individuals and identity holders. From this perspective, government, at least from a more global angle, is the most important role in identity theft prevention.

III. The legislative approaches which a government can take to prevent identity theft

1. The fundamental theory: Economic analysis of law

With respect to the reactions of an individual under certain circumstances, the

[42] United States Department of Justice: Identity Theft and Identity Fraud: What Should I Do To Avoid Becoming a Victim of Identity Theft? http://www.usdoj.gov/criminal/fraud/websites/idtheft.html. Accessed 6 Aug. 2008

[43] See Section V below.

economic model is an imperfect but persuasive one which can not only be used to explain an offender's action, but also predict the tendency of criminals, including the identity theft, in large scale. The basic economical model of criminal activities was proposed by Gray Becker[44], which seeks to explain the choices of criminals in legal and illegal activities. In his framework, one of the most important basic assumptions is that criminals, excepting committing crimes with passion, are rational and amoral. The rational criminal behavior can be explained by mathematical notation as follows[45]. Let the variable x represents the serious of the crime, y indicate the criminals benefits from the crime; the punishment f, and, the probability of being convicted is given by the function p. As we assume that the object of a rational, amoral criminal is to maximize his net benefits, the object can be shown as follows:

$$\max_x \pi(x) = y(x) - p(x)f(x)$$

This equation suggests the fact that increasing the probability of conviction, the severity of punishment or decrease the benefits of the offence could decrease the net benefits; accordingly, a rational and amoral criminal, who want to maximize his benefits, could incline to choose to act legally in this case.

The 'rational and amoral' assumption may be criticized in respect of the over simplicity, however, it can be used to explain and predict the criminal activities in a large scale. In fact, the above equation could be easily adapted to become a model of the quantity of crimes, rather than of one offender[46]. Instead of representing the seriousness of crimes, the variable x, now represents the aggregate number of crimes which is summing the number of crimes committed by each criminal in one society. Consequently, in the modified model in respect of cumulative offenders, an increasing in p or f, or a decreasing in y, will decrease the total number of crimes committed by rational and amoral offenders in the community[47].

The equation above with regard to offenders can be slightly adapted to predict or evaluate the behaviors of individuals, including the "identities holders". Generally speaking, this equation suggests that either an increasing of benefits or a decreasing of costs could offer incentive to individuals to complete object. On the contrary, a decreasing of benefits or an increasing of the costs may stop individuals to complete the object. As a result, for example, as to the identities holders in terms of identity theft prevention, taking measures to increase the costs of lost of identities is an effective way to induce identity holders to invest time and labors on identity theft

---

[44] Becker, G.: Crime and Punishment: An Economic Approach. 78(2) Journal of Political Economy P169-217 (1968).
[45] Cotter, R., Ulen, T.: Law and economics. Pearson Addison-Wesley. London (2008) P498.
[46] ibid 45, P499
[47] ibid 45, P500

prevention.

2. Approaches of preventing identity theft with respect to economic analysis

In light of the analysis above, there are three ideal ways to provide inducement for identity thieves not to commit crimes: an increasing of the seriousness of punishment, an increasing the probability of conviction of identity theft and depriving the payoff of identity theft. In fact, apart from these three approaches, there are still several general-purpose methods for crime prevention, such as the quality of arrest[48], the prevailing legal system[49] etc., however, they will not be discussed here because they are too general to identity theft prevention. The following discussions will focus on these three aspects.

At first, we have to notice that the probability of conviction and seriousness of punishment are not always independent to each other, in fact, as some empirical studies suggesting, server punishment, sometimes, potentially make the judge or jurors more reluctant to convict. The reason of this phenomenon is that when deciding whether or not to convict, jurors, even professional judges, take into account and try to find a balance of the cost of that they might convict an innocent person and the cost of acquitting a guilty person. If the cost of acquitting a guilty person rises, they are more likely to convict. On the other hand, if the cost of convicting an innocent person rises, they are less likely to convict. Because a more serious punishment increases the cost of convicting an innocent person, jurors or judges tend to take more serious standard to evaluate and review the evidences to lower the probability of conviction[50]. That is to say, merely increasing the scale of punishment could be on the risk of causing unpredictable and even contradict results. From this standpoint, a way can be deemed as a good one only if it can increase the gravity of punishment as long as keep the probability of conviction.

On the other hand, though an increasing of the probability of conviction may not result in the unwelcome side effect: decreasing of seriousness of punishment, however, even a tiny increasing of the probability of conviction requires a lot of resources allocated to the enforcement department, such as police and prosecutors; that is to say, it is very expensive in general[51].

Based on the foregoing grounds, a good approach to prevent identity theft is simultaneously increasing the probability of conviction and seriousness of punishment. The most obvious specific approach is criminalizing “identity theft”, especially

---

[48] Hirsch, W. Z.: Law and Economics: An Introductory Analysis. Academic Press. Boston (1988) P266.
[49] ibid. 48
[50] Mialon, H. M., Rubin, P. H.: The Economics of the bill of rights, Am. L. & Econ. 10(1) P40-79 (2008).
[51] ibid 45, P514

purposely filling some uncovered gaps in the legislations. That is to say, some kinds of activities in connection with "identity theft" should be punished under the new legislations. Comparing to Taiwan, the USA and the UK both introduced some statutory provisions to criminalize identity theft; both will be discussed in the following sections.

Additionally, with respect to the cost and severity of punishment, it has been shown that the fine is much cheaper than jail sentence[52] and, in general, the cost of wrongfully convict an innocent person with sole fine is much lower than with the jail sentence, therefore, jurors or judges will less reluctant to convict while only a larger fine is imposed. However, in terms of the seriousness of identity theft, only imposing fine may be not an appropriate instrument to prevent identity theft and, most importantly, a proper fine is not easy to decide. On these grounds, an appropriate "fine", which is proportionate to the wealth and to the benefits obtained from the offences, is a better instrument for identity theft prevention. Moreover, depriving benefits of offenders are an economic way to stop crimes, as we have seen before. From these perspectives, the confiscation and forfeiture scheme, especially in a relatively modern formation, is a suitable approach to prevent identity theft. In the following section, UK confiscation and forfeiture structure will be introduced, as it comprises a lot of features which are valuable, particularly, in terms of completely depriving the benefits of the offenders.

At last, in addition to the criminal legislations and forfeiture schemes, data protection laws are another way which could be used by the government to prevent identity theft. In general, a set of comprehensive data protection laws may impose data controllers, i.e. one type of identities holders, some obligations to enforce them to process identities more carefully; as a result, the identity thieves will be hampered because the cost of identity theft may rise as long as the benefits may be reduced. For example, the technology, such as phshing tracking and cryptology tools, which adopted by the data controllers can effectively block the phshing and spyware and fill the security leak. Because the EU and, accordingly, the UK have most comprehensive and thoughtful data protection schemes in the world[53], the provisions of UK's data protection legislations in connection with identity theft prevention will also be shown in the following sections. These provisions will also be illustrated in terms of the economic analysis mode. Moreover, even US data protection laws are not as complete as UK laws, with the rapid spread of identity theft; the US government has created a lot of data protection legislations to regulate data controllers in various specific areas, which

---

[52] ibid 45, P514

[53] Miller, M. Z.: Why European is safer from CHOICEPOINT. The George Washington International Law Review 39(2) P395 (2007).

will be also introduced in the following sections.

IV. New categories of offences in connection with identity theft

1. The UK approach: Fraud Act 2006

In past, a defrauder who used other's identities to create an account to obtain benefits would not be charged under the Theft Act, 1968 s. 15, because the benefits gained by the defendant would not be property belonged to another, a newly created debt in his own account instead. This loophole was closed by an amendment to the Theft Act, s. 15A. In addition, under the new Fraud Act 2006, this would now be a Section 2 (1) offence: there is no need to show that any property belonged to another was obtained[54]. In addition, phishers, which would not be charged in the past, could also be charged with this new section, as the explanatory points out: "This offence would also be committed by someone who engages in "phishing": i.e. where a person disseminates an email to large groups of people falsely representing that the email has been sent by a legitimate financial institution. The email prompts the reader to provide information such as credit card and bank account numbers so that the "phisher" can gain access to others' assets[55]". As a result, is can be seen that the section of this Act creates a widest form of the fraud offence and therefore likely to be the most frequently charged. The *actus reus* of this offence requires that the offender made a false representation, and that its *mens rea* is satisfied by evidence that he knew the representation is false and, he acted dishonestly and with the intent to gain and or cause loss[56].

However, Section 2(1), with regard to phishing, still leaves some uncertainties and difficulties that may impede its effectiveness. The most obvious one is that it only applies to offences in respect of fraud, or more specifically, of financial gain or losses. Therefore, phishers who collect confidential personal identity information for other purposes would not fall in the realm of this provision. Furthermore, this provision imposes the burden of proof on the prosecutor to prove that the defendant with "the intent to gain and cause loss". This burden may be hard in some circumstances, for example; it is difficult to prove the intent when the phishers are arrested prior to providing the information they unlawfully collected for defrauders. On this ground, the reverse burden of proof, imposing the burden of prove "no intention to gain or cause loss" on the defendants may be a practical solution.

2. The USA approach: ITADA

---

[54] Withey, C.: The fraud Act 2006-Some Early Observations and Comparisons with the Former Law. Journal of Criminal Law 71(3) P220-237 (2007)

[55] OPSI: Explanatory Notes to Fraud Act 2006. http://www.opsi.gov.uk/acts/acts2006/en/ukpgaen_20060035_en_1. Accessed 6 Aug. 2008.

[56] Ormerod, D.: The fraud Act 2006-Crimializing lying? Criminal Law Review. P193-219 (2007).

Comparing to the UK Act, the US legislators provide a wider criminal legislation to forbid identity theft. The most important criminal statue is the US Code Title 18 Section 1028, with the title "Identity Theft and Assumption Deterrence Act" (ITADA thereafter). The title suggests that the Congress hoped that this legislation will restrain the quickly rising tide of identity theft[57]. By 1998 when Congress passed this Act, the federal regulations in connection to prevention of identity theft are criticized as a jumble of laws[58]. For instance, there are some regulations involved the consumers' data only primarily to defend or improve accuracy of stored information and not to combat identity theft[59] and, instead of "all kinds of identities", there is a statute, 42 U.S.C. s. 408(a)(7)(B), provides that whoever- for purpose of obtaining anything of value from any person, or "for any other purpose" with intent to deceive- falsely represents a number to be the Social Security account number assigned by the commissioner to him, when the number is not assigned by the commissioner to him. In addition, with the severe situations of identity theft, many states pass laws specifically criminalizing identity theft[60]. The disadvantages of the previous legislation schemes are obvious: at first, the previous laws criminalized use of identification documents but not use of unprinted identification information[61]. Secondly, the scattered and board natures of regulations impede the work of prosecutor and other law enforcement[62]. Accordingly, a new act which purposely draws attention on identity theft is necessary.

The purpose of ITADA is criminalizing identity theft, and enables the law enforcement to target identity thieves earlier rather than waiting to charge thieves after they commit other offences with the stolen identities[63]. The instrument provided by this Act is strong penalty to deter identity thief. Specific activities prohibited include[64]:

— knowingly producing, transferring, or possessing an identification document, authentication feature, or a false identification document;

— knowingly producing, transferring, or possessing a document-making implement or authentication feature with the intent that it be used in producing a false identification document or another document-making implement or authentication feature which will be so used;

---

[57] McMahon, R. B.: After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevelent Crime in Amercia? 49(3) Vill. L. Rev. P625-660. (2004).

[58] ibid

[59] ibid

[60] ibid 57

[61] Hoar, B.: Identity Theft: The Crime of the New Millennium. http://www.cybercrime.gov/usamarch2001_3.htm. Accessed 6 Aug. 2008

[62] ibid 57

[63] ibid 57

[64] Jacobs, A. J., Surette E. C., 50 Am. Jur. 2d Larceny §62.

— knowingly transferring, possessing or using a means of identification of another person with the intent to commit or abet an unlawful activity; and
— knowingly trafficking in false or actual authentication features.
Furthermore, a specific statute outlaws "aggravated identity theft," stating that whoever, without lawful authority, during and in relation to any felony violations, knowingly transfers, possesses, or uses, a means of identification of another person is subject to sentence (s. 1028A(1)). The penalties are increased if the identity theft is in relation to a terrorism offense (s. 1028A(2)).
US ITADA provides a more comprehensive criminal instrument to prevent identity thief. According to the text in the statue, almost every type of acts in relation to unlawful identities is embraced.

To sum up, both the USA Act and the UK Fraud Act 2006 criminalize some types of identity theft which were free in the past, according to the economic analysis model above; the number of offences of identity theft will be lower as the costs of offences are higher and therefore, the identity theft will be deterred, theoretically at least.

V. Increasing the seriousness of punishment by depriving benefits of offenders

1. General Overview

On the grounds of the economic model above, depriving the benefits or profits from crimes is one of the most important measures on deterring criminals, because as comparing to the enormity of revenues derived from crimes, a loss of liberty through a term in a prison becomes an acceptable cost[65]. Identity theft, whether organized or individual, as a kind of crime involved interests, follows the ongoing rule: the fewer benefits, the fewer thieves. As a result, one of the effective and reasonable ways to prevent identity theft is depriving the benefits from criminal conducts of the identity thief.
Comparing the forfeiture schemes in the three countries, firstly, in the US, there are no unified forfeiture legislations; sparse forfeiture legislations mainly concentrate on specific crimes such as organization crimes[66] or drug trafficking[67], rather than general criminal conducts, including the identity theft. On the other hand, in Taiwan, based on

[65] Gallant, M. M., Money Laundering and the Proceeds of Crime. E. Elgar. Northampton (2005) P3.
[66] The Racketeer Influenced and Corrupt Organizations Act (18 U.S.C.A. § 1961-1968)
[67] 21 U.S.C.A. § 881

the s.38 of the Crime Code, all belongings which are benefited from offence conducts or used for offence conducts should be forfeited. The belongings here are restricted to be owned by the offenders, and restricted to the original ones; that is to say, as long as the offenders trade the belongings for money or other advantages, the benefits can not be removed from the offenders any more. Accordingly, the schemes of the US and Taiwan are too narrow and are not very useful in respect of identity theft prevention.

In contrast to the US and Taiwan, the forfeiture and confiscation scheme of the UK is more comprehensive and modern, as a result, in the following section, the forfeiture, or the confiscation legislations in the UK will be fully illustrated and exemplifies how forfeiture and confiscation scheme can prevent identity theft.

2. Confiscation order in the UK

(1) History

In the UK, "confiscation order" is the measure which can be adopted by the government or law enforcement to achieve the goal: depriving benefits from offenders in order to deter them. However, the confiscation scheme of the UK, in the past, were not acceptable, even "seriously under-utilized"[68]. As a result, a new "Proceeds of Crime Act 2002" (POCA, thereafter), which introduced a new agency and incorporated new and comprehensive schemes were introduced in 2002. The most important and most in deep connection with identity theft prevention parts are introduced in the following subsection.

(2) POCA

The confiscation proceedings in POCA can be roughly divided into four major stages[69], which are seen as follows:

The first one is deciding the defendant has a 'criminal lifestyle', which is a whole new concept introduced in POCA. A defendant with a 'criminal lifestyle' will be under unlimited and rigor historic investigation into his 'general criminal conduct'[70]. 'Criminal lifestyle' is so critical that it must be totally well defined rather uncertain: a defendant who is determined to qualified 'criminal lifestyle' as his conviction of offences falling within the statutory lists in POCA s. 75. There are three sub-categories: offences in Sch.2, offences which 'constitute conduct forming part of course of criminal activity' and an offence committed over a period of at least six months. The first category is consisting of several specific, or 'serious' from other perspectives, offences: drug trafficking, money laundering, terrorism, arm trafficking and etc. The last two categories can be viewed as that the defendant involved, at least suspiciously,

---

[68] PIU Report: Recovering the Proceeds of Crime. http://www.cabinetoffice.gov.uk/strategy/work_areas/~/media/assets/www.cabinetoffice.gov.uk/strategy/crime%20pdf.ashx. Accessed 2 Aug. 2008

[69] Rees, E., Fisher, R.: The Proceeds of Crime Act 2002 Oxford University Press. Oxford (2004) P30

[70] POCA s. 6(4)(a)

lives for crimes or, has a 'crime habit'. On these grounds, it is more reasonable to adopt a stricter standard in determining the amount of recovery proceeds.

The second stage focus on whether the defendant benefited from criminal conduct: only the offenders who are benefited from their offences should be deprived of benefits. The benefit here includes property and pecuniary advantage[71], more specially, the value of the property and a sum of money equal to the value of the advantage. As long as the defendant does actually obtain the property, he need only do so momentarily[72].

The third stage is determining the recovery amount. This is a complex stage, when failures and misunderstandings often appear without any "professional assistances". The prosecutor in this stage has to prove, under the civil burden of proof[73], the total amount of benefits gained by the offenders. Some offenders', especially the offenders with "criminal lifestyle", criminal history may last long and involve complex financial transactions which may impede the court to uncover the real benefits from the offences concerned. To resolve the difficulties, the POCA, following the DTA, introduced several assumptions[74], which, in general, make an assumption that all benefits obtained by a "criminal life" offender within a fixed time interval are in connection with the offences concerned. The offender, when the assumption are applied, is imposed a burden to prove that these benefits do not result from criminal conducts; otherwise all these benefits constitute the recovery amount. However, the court has a discretion power to make no assumption while the assumptions are incorrect or injustice[75].

The last stage is determining the available amount. It is the stage of importance and with the most controversies[76], because the court can not confiscate more than the defendant is worth, that is to say, the defendant should only be enforced to pay the available amount. In POCA s. 9, the 'available amount' is the aggregate of: the total of the values of 'all the free property then held by the defendant minus the total amount payable in pursuance of obligations which then have priority', and the total of the values of all 'tainted gifts': the 'gift' is defined as 'significantly less than the value of the property at the time of the transfer'and the gift whether should be deemed as 'tainted'variously depends on whether the defendat has a criminal lifestyle[77]. So far the burden of proof in the confiscation proceedings, in general, has been on the prosecutor. However, in the last stage, as long as the prosecutor discharge the

---

[71] POCA s. 76
[72] R v Patel [2002] 2 Cr App R(S) 10.
[73] POCA, s. 6(7)
[74] POCA s.10
[75] POCA s.10(6)
[76] ibid 69 P45
[77] POCA s. 77

defendant obtained benefits from his criminal conducts and the recovery amount, it is the defendant's burden to prove the available, or the realized amount of his assets is less than the amount of his benefits[78]. The prosecutor has no burden to submit a prima faice case once the prosecutor has established the existence of benefits[79]. Therefore, in practice, the reverse burden of proof in accompany with the suspicious 'hidden assets' make the defendant hard to utilize this upper bound to relief his obligation. For example, in R v. Wright[80], the court of Appeal (Phil LJ) indicated: 'Of course there are many ways in which assets can be hidden, including assets being held temporarily some other person on the defendant's behalf. The burden was on the appellant, an appellant who hitherto had a lavish lifestyle. It was for the judge to form a judgment on realized assets in those circumstances'.

(3) Rational

The justifications behind confiscation orders are varied in many cases, in Glatt[81], the court lists a through consideration of case law and makes a conclusion of it[82]:

a. Confiscation orders are a penalty and are a measure to which Article 1 of Protocol of the ECHR is applicable[83].
b. Confiscation orders are designed to deter those who consider starting offences[84].
c. Confiscation orders are used to deprive a person of benefits received from criminal conducts and to remove the value of the value of the proceeds derived from criminal conducts from future possible criminal use[85]. However, confiscation orders are designed essentially to impoverish defendants, not to enrich the Crown[86].

To sum up, case laws indicate that the confiscation order can be seen as a fine which is designed to deprive the benefits of the offenders and accordingly, deter him to conduct future offences. From this perspective, the fine, including the confiscation, is often regarded as the most efficient type of punishment. The reasons are not only that the imprisonment is very expensive, but also the impairment of the offenders' skills in the course of imprisonment[87]. Moreover, one of the drawbacks of fine is that the fine, as usual, which is no relation to various wealth and income of individual offender, may

---

78 R v. Comiskey [1991] 93 Cr App R 277.
79 R v. Barnham [2005] EWCA Crim. 1049
80 R v. Wright [2006] EWCA Crim 1257
81 R. v Louis Glatt [2006] EWCA Crim 605
82 Millington, T., Williams, M.S.: The proceeds of crime : the law and practice of restraint, confiscation, and forfeiture Oxford University Press. Oxford (2007) P181.
83 Welch v United Kingdom (A/307-A) (1995) 20 E.H.R.R. 247
84 R v Rezvi (2002) 2 Cr App R(S) 70
85 Re T (Restraint Order; Disclosure of Assets) [1992] 1 WLR 949
86 Re P [2000] 1 WLR 473
87 Posner, R.A.: Economic Analysis of Law. Little, Brown (2003) P223.

finally impose prison sentences on criminal without ability of payment[88]. The proportionate confiscation, according to the proceeds benefited from the criminal conducts, is a proper mechanism which can be adopted to reconcile both the cons and pros above. As we have seen above, a lot of quite comprehensive measures, for instance, the assumptions of benefits obtained from offences, are introduced in the POCA 2002, which should be very essential and critical to prevent identity theft.

3. Forfeiture order in the UK

Powers of forfeiture of the objects of offences are easily found in much statuary: unlawful firearms (Firearms Act 1968 s. 52), knives (Knives Act 1997 s.6) and even aircrafts in connection with unlawful immigrations (Immigration Act 1971 s. 25C). Counterfeit coins and tools for making forgeries or false instrument are able to be forfeit by magistrates with a conviction (Forgery and Counterfeiting Act 1981 s. 7, s.24). A more general regulation about forfeiture is introduced in the section 143 of the Powers of Criminal Courts (Sentencing) Act 2000, which, is the case where a conviction has been made, grant the court a power to forfeit any interest which the offender has in property that was used or intended to be used for committing or facilitating the commission of any offences; therefore, a vehicle used in disqualifying driver could be forfeited under this section[89]. Property was only seized under this section if it was in the possession or control of the offender at the time of his arrest[90]. To sum up, the objects of forfeiture can be divided in two categories: the first one is the items are objects of crimes, such as the guns in the offence of unlawful possession of firearms; the second one is the instruments of crimes, such as the knife in a murder, and the vehicle in a man-slaughter car accident[91].

(2) Rational

To justify forfeiture is not as clear as confiscation and, accordingly, is worth more concerning. The most obvious justification of forfeiture is regarding it as a fine. Nevertheless, this concept is a bold one, especially in regard to a few clear flaws of it[92]. The second justifying reason is preventing future crimes, but this reason does not perfectly justify the seizure of an item which has a wide range of lawful usage[93].

Comparing to confiscation order, the forfeiture, in the first glance, seems to have no such direct connection with depriving gains from the defrauders. However, considering the main justifying reasons above, forfeiture definitely is an effective approach of preventing identity thief. At first, forfeiture, as a fine, actually deprives

---

[88] ibid.
[89] Regina v Highbury Corner Metropolitan Stipendiary Magistrate [1992] 1 All ER 102
[90] Alldridge, P.: Money Laundering Law. Oxford University Press Oxford (2003) P110
[91] ibid P61
[92] ibid 90 P60
[93] ibid 90 P61

the economic gain of the identity thief. Secondly, seizure of instruments which can be used to committing further crimes is raising the cost of future offences as long as reducing the incomes from the committed offences.

4. Conclusion

The rationales of recovery of criminal proceeds, including confiscation and forfeiture, are generally as follows[94]: show that crime will pay eventually and underpin confidence in a fair and effective criminal justice system; remove negative role models from communities; disrupt criminal networks and markets with an impact on volume crime; deter people from crime by reducing the returns that can be anticipated; improve crime detection rates generally by providing a deeper understanding of criminal markets and assist in the fight against money laundering and the harm that it causes. All these rationales, under the foregoing economic model, suggest that an effective mechanism of proceeds recovery can successfully deter and reduce the identity theft.

VI. The UK and US data protection legislations in respect of identity theft prevention

1. UK legislations

(1) Introduction

With regard to the specificity, the regulations or the obligations cast upon the data controllers or identity holders by UK data protection legislations may be divided into two categories, the first one, the general regulations, are used to enforce the data controllers to carefully process identities but without any explicit directions. On the contrary, the specific ones, the regulations of this type are clearer and, the identity holders which follow the specific directions set up by these regulations could avoid the loss caused by identity theft, including the loss of victims as well as the liability of identifies holders. The legislations of these two types are illustrated as follows.

(2) Specific regulations in respect of identity theft prevention

The Principle 7 of Data Protection Act 1998 mandates the data controllers and identity holders should use technology to safeguard the security of confidential information possessed by them. This principle indicates a direction which identity holders should follow to defend identity thieves; however, as we know, it does not insist any specific technology. On this grounds, the identity holders, especially the intuitions covered by this principle, could take any effective and economic technical solutions they want to deal with the identity theft.

---

[94] ibid 68 P17

For instance, in terms of anti-phishing, technical measures are as important as the foregoing legislations because technical tools can directly detect the phony websites or, prevent Internet users from accessing to the phony websites. The present popular anti-phishing solutions fall into two board categories: site badges and phishing indicators. The Passmark SiteKey[95] and Yahoo's sign-in seal[96] are two common measures belonged to the site badges. The Passmarks SiteKey, which is adopted by the Bank of American to communicate to its 13 millions customers, combines two passwords and other authentication mechanisms to identity the users[97]. The images of each site will be different while users use different computer to access to the site[98]. On the contrary, the Yahoo Sign-in Seal is associated with a browser rather with a user's account. More important, the Sign-in Seal is based on personal pictures, not with images offered by sites, which is intended to increase familiarity for the uers, and reduce the risk of phishing accordingly[99]. In addition, phishing indicators are toolbars embedded in browsers which try to evaluate, detect and separate suspicious websites and thus protect users on the Internet[100]. In terms of spyware, many companies provide software or packages to defeat spyware, and some are free. Some ISPs, like AOL, provide spyware protection services for their users[101]. To sum up, identity holders that want to lessen liability of identity loss should take any effective and practical technical measures which are useful in identity theft prevention.

(3) General—liability

As we have seen in the economic model of individual's decision, the goal of a reasonable man is seeking to maximize his benefits, that is to say, when an individual is at risk of loss, he will pay more attention and spend more time to avoid the loss happening. On this ground, the s. 61 in Data Protection Act 1998 could be a useful instrument to prevent identity theft. Under s. 61, a director, manager secretary or other similar officers of a body corporate and the body corporate itself may be liable while the employees of this body corporate were convicted of offences under this act, as long as the director etc. must involved in the offence by virtue of some connivance or neglect[102]. Based on this section, the officers, who take the main responsibility of an

---

[95] RSA: RSA: Consumers' solution http://www.rsa.com/node.aspx?id=3072 Accessed 6 July 2008

[96] Yahoo: Give password scams the boot with personalized sign-in seals https://protect.login.yahoo.com/. Accessed 6 July 2008

[97] Bauknight, T.: PassMark's SiteKey - Answering The Wrong Question http://www.webpronews.com/node/21549/print. Accessed 6 July 2008

[98] Agarwal, N., Renfro S., Bejar, A.: Phishing Forbidden. 5(5) ACM Queue P28-33 (2007)

[99] ibid.

[100] ibid

[101] InfoWorld: AOL adds spyware protection. http://www.infoworld.com/article/04/01/06/HNaolspyware_1.html. Accessed 6 July 2008

[102] Carey, P.: Data Protection: a practical guide to UK and EU law. Oxford University Press. Oxford (2004) P195

identity holder, should process the identities more carefully since they want to avoid the potential loss resulted from identity theft, which is his own direct risk in this case, not the irrelevant loss of victims.

2. US legislations

(1) Introduction

Comparing to the data protection laws of the UK, US laws, at least in the Federal level, has not introduced a comprehensive data protection scheme, rather, the US legislators impose various obligations on different kind of identity holders, such as health care institutions[103] (The Health Insurance Portability and Accountability Act, HIPAA thereafter), financial institutions[104] (Gramm-Leach-Blily Act, GLBA thereafter) and credit report agencies[105] (Fair Credit Reporting Act, FCRA thereafter). With regard to identity theft, the guidance introduced by these legislations is mixed; that is to say, some are specific and others are rather general. Therefore, it is easier to illustrate these laws respectively, rather than categorize them as specific or general.

(2) HIPAA

HIPAA is a federal law which creates obligations of health providers and other related institutions. It attempted to address the privacy of personal health information by banning the disclosure of individually identifiable health information without the patient's prior consent[106]; the 'individually identifiable health information' is a subset of health information which is created or received by a health care provider, employer, or health care clearinghouse; and relates to the past, present, or future health of an individual and can be used to identity an individual[107]. In terms of identity theft prevention, HIPAA and related regulations provide technical, physical and administrative safeguards to protect the protected health information against unlawful access and to ensure the health institutions which want to use the information for the purposes other than treatment or payment should obtain the written authorization in advance[108].

In fact, HIPAA does not only influence the health care industry and law enforcement, but the IT industry as well. Even though identity theft prevention is not the original target, at least not the main one, of HIPAA, the practical effectiveness shows that this legislation can actually prevent the identity theft to some extents. At first, the health care institutions are one of the few leaks of children identities, since most children do not have any credits reports, banking accounts or other related official records; that is

---

[103] 42 U.S.C. 1320
[104] Pub. L. No. 106-102, 113 Stat. 1338
[105] 15 U.S.C. 1681-1681t, Fair and Accurate Credit Transactions Act (FACTA) 15 U.S.C. 1681 et seq.
[106] ibid 9
[107] Gerard, G. J., Hillison, W., Carl, P. Identity theft: the US legal environment and organizations' related responsibilities. 12(1) Journal of Financial Crime P33-43 (2004)
[108] ibid 106

to say, health information is the only source of children identities. Secondly, excepts the social security numbers and other financial identities in relation to credit cards, identity thieves also steal health identities, such as health plan numbers, from doctors or hospital's offices as well as government funded insurance numbers from medical programs and use these stolen identities to forge the faked medical bills for the insurance companies for payment[109]. Nevertheless, according to a report as many as 250,000 to 500,000 Americans have had their identities stolen from their heath care records which contain personal and confidential information[110].

(3) GLBA

GLBA, Financial Services Modernization Act, provides serveral modernazation which is desired by the insurance and banking companies, targets the protection of private consumer information by financial intituations as well. The section Fraudulent Access to Financial Information (FAFI thereafter)[111] of GLBA is in relation to pretexting, which is the act of creating and using an invented scenario (the pretext) to persuade a targeted victim to release information or perform an action and is done by phone, emails and even by phony websites (phishing in the case). The GLBA forbid pretexting by encouraging the organizations covered by the GLBA to implement programs fulfilling GLBA's Safeguards Rule[112]. The GLBA Safeguard Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect the security and confidentiality of clients' nonpublic personal information. (In addition, it applies to information of those no longer consumers of the financial institution as well)[113]. Under GLBA, the Privacy Rule governs the financial instituations to have to give notices to inform the customers what the informaton gathering from them and what is the privacy policy of the institutions prior to the customers entering into the contracts[114].

(4) FCRA and FACTA

The legislations above, no matter providing what kinds of protection, concentrate on the prevention prior to identity thefts occurs. However, even after the identity theft has appears, the subsequent assistance provided for the victims is still very essential to identity theft prevention, because the subsequent steps could help the victims to recover their reputation, effectively limit further losses of victims and, more

---

[109] Miller, S. A.: Identity Theft And The HIPAA Regulation http://www.fepblue.org/privacyhipaa/privacyhipaaidentity.html. Accessed 1 Aug 2008

[110] ibid

[111] 15 U.S.C. 6801-6827

[112] 15 U.S.C. § 6801–6809

[113] Wikipedia: Gramm-Leach-Blily Act http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act. Accessed 1 Aug 2008

[114] ibid

importantly, may forbid thieves using identities from the same source to commit more crimes.

On theses grounds, several helps for identity theft victims are incorporated into FCRA and its amendment FACTA. Firstly, under FACTA, a victim has a right to contact a credit reporting agencies to set up "Fraud Alerts" on his credit files of the major credit bureaus. When creditors assess the credit before making a new loan they see the fraud alert and are required to confirm identity before making the loan at a telephone number provided. Secondly, a victim has right to claim a copies of applications for credit or transaction records to understand the whole frauds. Both measures provided have practical influences on identity theft prevention.

(5) SSMPA

Social security numbers are the most common targets of identity thieves and therefore, US legislators introduce Social Security Misuse Prevention Act (SSMPA) to prevent identity theft. The main target of this act is banning the sale and display of individuals' social security numbers without the identity holder's prior consents[115].

VII Criticizing the Taiwan government's legislative strategies for identity theft prevention in respect of the three kinds of legislations

The three kinds of legislations which could be used to prevent identity theft have been illustrated in the foregoing sections. Comparing to Taiwan, the US and the UK, although with some drawbacks, have relatively comprehensive and effective legal schemes.

At first, in terms of the criminal codes, in Taiwan, there is no specific offence for identity theft. Rather, fraudulence[116], the common outcome of identity theft, and criminalized invasion of computer system[117], the technical precursor of identity theft, are the general weapons offered for the police and persecutors against identity theft. From this standpoint, an identity thief who has successfully obtained identities but has no chance to use the identities to commit other crimes, such as fraudulence, is totally legally free, as long as he does not violate other offences in the course of obtaining

[115] U.S. SENATOR PATRICK LEAHY: Lawmakers Target Identity Theft In New Bill http://leahy.senate.gov/press/200301/012703.html Accessed 1 Aug 2008

[116] Crime Code s. 339

[117] Crime Code s. 358

identities. Moreover, with regard to the identity traders, conspiracy with defrauder or identity thief is far inadequate, especially when neither defrauder nor identity thief is present in the case.

Secondly, the forfeiture scheme in Taiwan is quite conventional, to speak more clearly and directly, is quite old-fashioned. The chapter of forfeiture and confiscation in Taiwan Crime Code has not been adapted since 1930, the time when it was enacted. As a result, not surprisingly, the forfeiture scheme can not provide sufficient assistances in effectively depriving benefits from offenders. For example, real property and pecuniary advantages are not targets of forfeiture and, more importantly, complete and wide confiscation of proceeds is merely incorporated in specific offences, such as corruption[118], drug trafficking[119] and organized crimes[120] etc. That is to say, benefits of offences are not easily deprived from identity thieves; accordingly, the deterrence of identity theft solely could depend on imprisonment, which has been proved cost and ineffective.

At last, with regard to data protection regulations, Taiwan's data protection act, which was enacted in 1995, has not adapted since then and the concentration of this Act is generally on officials; the private identities holders, such as commercial banks and marketing sections are not embraced. In other words, a big identity leak appears in this Act.

On these grounds, the prevention measures in respect of legislations in Taiwan are considerably inadequately, incomprehensive and ineffective; more laborious work is needed in order to shorten the distance behind the UK and the US.

VIII. Summary and Suggestions

Identity theft gradually widely spreads today, ironically, according to empirical evidence; identity theft is affiliated to modern society and, in other words: a more modern society suffers more serious identity theft. The reason of this phenomenon is that identity theft relies on, to some extents, loose connections between people in a modern world. A village where all residents know each other well is not a good forcing house of identity theft. Moreover, new communication technologies, such as the Internet, foster identity theft as well because each one, if he wishes, could have a new and totally different 'identity' on the Internet[121]. To sum up, Identity theft is a critical problem which has to be resolved in modern societies.

In respect of prevention of identity theft, legislative measures of three different aspects

[118] Anti-corruption Act s. 10
[119] Drug Trafficking Act s.19
[120] Organized Crime Act s. 43
[121] ibid 1

have been proposed in this article: special offences in crime codes, benefits deprivation legislations and data protection laws. Unfortunately, Taiwan, compared to the UK and the US, is deficient in all of these three aspects. The main reason of this ignoring and lacking may be result from the priority of the Taiwan government and, with regard to political reality; the priority is definitely a mirror of popular concern and interest. Up to now, the popular concern in Taiwan focuses on other offences rather than identity theft. However, as we have illustrated in section II, in Taiwan, some kinds of frauds, such as false representation frauds, in fact, are in deep relation to identity theft. In addition, adoption of newer technologies as well as incorporation of a more modern financial system will eventually provoke serious identity theft in Taiwan. On these grounds, a more comprehensive, especially in respect of the legislative measures of all these three aspects are more and more necessary for Taiwan. However, although these three measures are all mainly in connection with legislations, the difficulties and costs of them are not equal. Comparing to the other two, data protection laws are cheapest and, the comprehensive forfeiture and confiscation schemes need most investments, embracing time as well as money. As a result, a set of comprehensive data protection legislations should be a strategy with the highest priority, especially with regard to economic factors.

Except of these three kinds of measures which government could use to protect victims from identity thieves, there are several innovative ways of legislations which combing technology and legal aspects could also be adopted. For example, with regard to prevention of spyware, because the issuer or designer of a software is its most important identity and software users should have full information of it before making decisions about what software should reside in his machine; as result, a set of legislations, which imposes the software design houses an obligation of offering readily identifies and lets the users have full freedom to uninstall or remove the installed software, is very critical to users as they can employed these identities to assess the risk prior to installment[122]. As to the technical factors, the technology of this suggestion is easy and in fact, some kinds of software, such as open source software[123] and Creative Common software[124], enforce redistributors and modifiers to keep the whole license information, including the designers' names.

In summary, the identity theft is one of the most significant problems in the UK, the US as well as Taiwan. All governments shall pay more attention in coping with it and,

---

[122] Thompson, R.: Why spyware poses multiple threats to security 48(8) Communication of ACM. P41-43 (2005).

[123] GNU: GNU General Public License http://www.gnu.org/licenses/gpl-3.0.html. Accessed 1 Aug 2008

[124] Creative Commons: Creative Commons Attribution 3.0 http://creativecommons.org/licenses/by/3.0. Accessed 1 Aug 2008

based on the above economic model, legislations, which can only be mandated by government, are powerful weapons against identity theft. Every government among the above three actually has some progresses in this aspect, but, Taiwan in particular, has to do more. Furthermore, the analysis and the suggestions in this article are just a beginning; further researches are needed in the future.