RJSH Vol. 2, No. 1, January - June 2015, pp.85-93

Data Breach Notification Laws as a Preventive Approach to Identity-Related Crimes: Lessons from the US for Thailand's Data Privacy Laws

KanathipThongraweewong

Faculty of Law, Saint John's University, Thailand
Email: kanathip@yahoo.com

Submitted 12 October 2014; accepted in final form 13 November 2014

Abstract

Private sector organizations have increasingly collected the personal data of their customers in the course of conducting business. However, "data breach" can occur in cases of unauthorized access to personal data stored by business entities. The breach can lead to cybercrimes such as identity theft, identity fraud and identity-related crimes resulting in financial and reputational losses for both firms and customers. In response to data breach events, several U.S. states have enacted statutes or specific laws imposing responsibilities on firms to notify their customers when a data breach occurs. Although there are negative effects, data breach notification laws lead to positive results for both firms and individual customers. For instance, these laws cause firms to take preventive measures to protect personal data. In addition, they enable individuals to be aware of a breach and take preventive measures of their own that could reduce identity-related crimes. Contrary to these state laws, this paper found that Thailand's legal system provides no specific laws regarding "data breach notification". Although Thailand has several laws relating to the protection of personal data, e.g., the Credit Information Business Act and the Official Information Act, this paper indicates that these laws are insufficient and inappropriate as a preventive approach to identity-related crimes. Thus, this paper's main recommendation is to propose the enactment of a specific law that incorporates a "data breach notification" principle by using the state laws of the U.S. as a model to protect the right to privacy in case of personal data being abused by identity-related criminals.

Keywords: *identity theft, personal data, data breach, data security, US data breach notification, Thailand laws*

1. Introduction

Private organizations, and business entities in particular, have collected and maintained vast amounts of personal information including names, identification numbers, credit card numbers and other information associated with the name that can identify each person. Data breaches can occur during unauthorized access to the data, including when such data are accidentally lost or intentionally stolen. A breach can lead to other cybercrimes such as identity theft, identity fraud and identity-related crimes resulting in financial and reputational losses for both customers and business entities. The legal domain offers two levels of protection. The first level involves laws that impose responsibilities on firms and entities that collect personal information to disclose publicly or to notify individuals of unauthorized access to their personal information. These laws can be regarded as a "preventive approach" because notification can enable individuals to take action to prevent any impact from identity theft, identity fraud and identity-related crimes. For example, individuals may close financial accounts, change passwords for electronic financial services and have credit cards reissued with new numbers. These laws can be applied to firms or business entities at a deterrent stage, i.e., before identity-related crimes have been committed. In addition, laws exist that proscribe identity-related crime when it actually happens. Thus, the second level involves laws defining what constitutes an identity-related crime and imposes liability on the one who commits such a crime. Laws on this level can be considered as a "proactive approach".

As for the preventive stage, several U.S. states have enacted specific laws referred to as "data breach notification or data breach disclosure". Regarding the proactive stage, specific laws regulate identity-related crimes when personal data are abused or used to facilitate other crimes. On the contrary, this paper found that currently the Thai legal system provides insufficient protection on both levels. There is no law that specifies "identity theft" or "identity-related crimes" as specific criminal offences. In addition, no law imposes specific responsibilities on businesses that collect personal data to inform individuals when

their data are lost or stolen. However, this paper's scope is limited to discussing only the first level of protection; laws imposing liability for identity-related crimes are excluded from analysis. Hence, this paper focuses on the preventive approach by studying U.S. "data breach notification" laws and comparing such laws with current Thai statutes. This could lead to suggestions related to the enactment and amendment of Thai laws to protect personal information from identity-related crimes. Therefore, the paper will review literature on identity theft, identity fraud and identity-related crimes and their impact on e-businesses and the financial sector. Then this paper will study the U.S. data breach notification laws and compare them with Thailand's statutes.

2. Methodology

This paper is conducted with the aim of studying the application and interpretation of data breach notification laws in the United States which enacted to protect individuals from potential identity-related crimes. The qualitative method is introduced. The scope of analysis includes examining related documents, i.e., U.S. state laws, as well as court cases and opinions of legal scholars. Such documents are analyzed by employing the content analysis method. In addition, comparative analysis is conducted by comparing the U.S. state laws with the relevant Thai statutes.

3. Identity Theft, Identity Fraud and Identity-Related Crimes

The increasing use of personal information to make important decisions and the widespread transfer of information among a variety of public and private organizations facilitate identity theft to a much greater degree than traditional ways of privacy violation (Solove, 1997).Regarding "identity-related crimes", three terms, "identity theft", "identity fraud" and "identity crime" are interchangeably used in many countries despite their having differing characteristics (McNally et al., 2008).

The first term, identity theft, is basically regarded as a crime of stealing personal information to commit a range of further offences including various types of fraud (Jewkes,2010).The Organization for Economic Cooperation and Development (OECD) defines it as an illegal activity of "acquiring, transferring, possessing, or using personal information of a natural or legal person in an unauthorized manner with the intent to commit, or in connection with, fraud or other crimes"(OECD,2008). In the United States, a federal law proscribing "identity theft" is the U.S. Identity Theft and Assumption Deterrence Act (title 18, s. 1028 (a) (7) U.S.C.). This law imposes liability on anyone who "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law". In Europe, Mitchison et al. (2004) demonstrated that it occurs "when one person obtains data or documents belonging to another,or the victim, and then passes himself off as the victim." Consequently, there are two main limitations regarding the scope of identity theft. Firstly, it covers only the abuse of a real person's identifying data. Koops and Leenes (2006) argued that the scope of identity theft is a narrow view because it covers only the unlawful use of identifying data from another person. However, some crimes can be committed without "stealing someone else's identity. For example, credit-card fraud can also be committed by generating a non-existing credit-card number". Secondly, identity theft is regarded as a subsidiary crime whereby identifying personal data are abused to commit another crime. In other words, the act of accessing or stealing data does not constitute a crime until another crime is committed.

Compared with identity theft, which is limited only to the theft of a person's identifying data, identity fraud has a broader scope because it includes the fraudulent use of any identity, real or fictitious. (Europol, 2006) A study by the UK Cabinet Office also demonstrated that "Identity fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent" (UK Cabinet Office, 2002). Thus, using a fabricated identity of a non-existing person falls under the scope of identity fraud.

Identity-related crimes have broader scope, covering both identity theft and identity fraud because this category "concerns all punishable activities that have identity as a target or a principal tool" (Koops and Leenes, 2006). In this paper, the term "identity-related crimes" is used to cover all activities that target personal identity. Nevertheless, this paper's scope is limited to preventive legal measures in the stage before

such crimes have been committed. Thus, the discussion of laws penalizing identity-related crimes is beyond this study's scope.

4. The Impact of Identity Theft on E-businesses and the Financial Sector

Identity theft is a critical concern for financial institutions, other business sectors and their customers around the world. A consumer survey by the U.S. Federal Trade Commission revealed that 8.3 million people were identity-theft victims in 2005 with total losses of $15.6 billion (Conkey, 2007). Apart from financial losses of victims, this crime causes other losses such as time spent resolving problems that arise. Barker et al. (2008) found that it takes years to restore the damage done to an individual's credit ruined. In addition, Listerman and Romesberg (2009) also indicated that it takes an identity-theft victim an average of 58 to 231 hours of personal time to deal with all of the correcting and legal issues. Further damage from identity theft, identity fraud and other cybercrimes spreads to customers' growing distrust in modern payment methods, e.g., credit cards, online payments and electronic banking, which can lead customers to change their behavior of payments (Benton et al., 2007;Jonker 2007). Arango and Taylor (2009) also confirmed that perceived risk is a strong driver of consumer decisions in payment methods. As a result, customers may switch to less efficient payment forms such as cash (Cheney, 2010;Arango et al., 2011).The AARP Public Policy Institute found that 24 percent of its survey's respondents said they always pay restaurant bills with cash rather than debit or credit cards because they are worried about their cards being misused (Mayer, 2009). This perception could have a negative impact on the growth of the online business industry. Sproule and Archer (2010) found that 20% of participants in a Canadian Survey of Payments, who had been victims of fraud, stopped or reduced online shopping, and 9% stopped or reduced online banking activities. In addition, when consumers avoid modern payment and credit tools out of such fear, they can distort and restrict consumption, thus sending misleading signals throughout the economy (Crooks, 2004). Consequently, identity theft, identity-related crimes and other cybercrimes are critical obstacles to the expansion of online businesses and the financial sector. As for prevention through a technological approach, sophisticated payment instruments, such as smart cards (Sullivan, 2008) and EMV chip technology developed by VISA (VISA, 2011), were developed to restore consumer confidence. As for promoting prevention through legal means, this paper will explore U.S.data breach notification laws and compare them with Thailand's statutes.

5. Result

The results can be divided into three main findings.

5.1The U.S. data breach notification laws

According to the content analysis, this paper has findings on the data breach notification laws of the U.S. states as follows:

- The paper found that most U.S. states enacted statutes inhibiting data breach by imposing responsibilities on firms that collect personal data to notify individuals that unauthorized access to their personal information had occurred.
- The paper indicates that the content and element of data breach notification laws varies among states. For example, each state's law has its own definition of "personal information".
- The paper indicates that an important exception to data breach laws is that they exclude information that is available to the public.
- The paper indicates that the threshold requiring notification varies among states depending on two different concepts: the "strict liability model" and the "risk assessment model".
- According to a majority of statutes, the critical element for notification requirement is the resident of victim, not the location of the firms or the breach.

5.2 The impact of data breach notification laws

Regarding the impact of data breach notification laws, this paper indicates that these laws affect both firms and their customers as follows:

- With regard to the firms, this paper argues that a notification requirement can affect a breached firm positively and negatively.
- As for the impact on individual, this paper argues that notification is regarded as a measure to ensure "the right to know" of individuals. In addition, notification can lead individuals to make decisions regarding the protection of their personal data.
- The paper argues that positive effects of data breach notification on both firms and their customers could lead to a reduction in identity-related crimes.

5.3 The comparative study of U.S. and Thai laws

According to the comparative study of U.S. and Thai-related laws, the main findings are as follows:

In contrast to what exists in the U.S., the paper found that Thailand's current legal system provides no specific laws regarding "data breach notification".

Although Thailand has several laws related to the protection of personal data,e.g., the Credit Information Business Act and the Official Information Act, the paper indicates that these laws are insufficient and inappropriate as preventive approaches to identity-related crimes.

6. Discussion

The results of the content analysis are divided into three parts as follows:

6.1 The US data breach notification laws

Several U.S. states enacted statutes regulating data breach by imposing responsibilities on firms that collect personal data to notify individuals that an unauthorized access occurred to their personal information. Although most states enacted statutes based on the law approved in California, which was the first state to enact a data breach notification law, the content and element of data breach notification varies across states.

The scope of "personal information" differs among statutes. For example, California law defines personal information as "a person's first name…and his or her last name in combination with any one or more of the following pieces of data, when either the name or the data elements are not encrypted or redacted: social security number, driver's license number or state identification card number, account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account" (California Civil Code, section 1798.82). In 2007, two more elements were added to the definition: medical and health insurance information (California Civil Code, section 1798.29 (e) (4)-(5)).However, several states have added elements to their definitions ; for example, Wisconsin and Iowa include "unique biometric data, including fingerprint, voice print, retina or iris image" (Wisconsin Statutes Annotated, section 134.98; Iowa Code Annotated, section 715 C.1(11)). North Carolina includes an employee's digital signature (North Carolina Statutes Annotated, section 75-65). New York broadly defines the term to include "any information concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person" (New York General Business Law, section 899-aa(1)(a)). Regarding the nature of data, most states focus on the breach of electronic or computerized data. However, some states, such as Alaska, Indiana and Wisconsin, include both written and electronic data.

As for exceptions, most states, similar to California law, exclude information available to the public from the definition of "personal information". For example, Indiana law provides that "the term does not include information that is lawfully obtained from publicly available information…" (Indiana Code Annotated, section 24-4.9-2-10). Alaska law states that "the term does not include publicly available information containing names, address, telephone numbers, or other information an individual has voluntarily consented to have publicly disseminated"(Alaska Statutes, section 45.48.590 (5)). Ohio law also provides that "personal information does not include publicly available information…" (Ohio Revision Code Annotated, section 1349.19 (A) (7) (b)). Utah law provides that the term "does not include information regardless of its source…in widely distributed media that are lawfully made available to the general public" (Utah Code Annotated, section 13-44-102(3) (b)).

Although most state laws require notification when there is a breach related to personal information, the critical difference among state laws is the definition of data "breach". In other words, the threshold requiring notification varies across states depending on two concepts: the "strict liability model" and the"risk assessment model".

With regard to the strict liability model, a firm is required to notify whether or not there has been actual damage to customers. In other words, even though an identity-related crime may or may not have been committed, a firm must issue notification of a data breach. Several statutes define "breach" as "unauthorized access" to personal data. For example, California law defines a breach as "unauthorized acquisition" of data (California Civil Code, section 1798.82 (d)).North Dakota law also defines a security breach as "unauthorized access to" or "acquisition of" computerized data (North Dakota Code, section 51-30-01 (1)). Other states that fall within this model are Arizona, Delaware, Florida, Illinois and Texas.

Contrary to the strict liability model, the "risk assessment model" requires breached firms to notify only under certain conditions, particularly when a risk assessment or investigation has been done to demonstrate the risk of a breach to individuals. Some states, such as Kansas, Maine, New Hampshire and Utah, require firms to determine whether there has been a misuse of personal data. Other states, such as Alaska, Arkansas and Florida, provide that notification is not required if a firm has conducted an "appropriate investigation" and "reasonably" determined that such breach has not and will likely not affect individuals. However, these laws require firms to create and maintain documents related to the investigation. Some states such as New York provide certain factors for firms to consider in determining a breach, e.g., (1) indication that an unauthorized person has physical control of the information through means such as a lost or stolen computer, and (2) the data has been download or copied (New York General Business Law, section 899-aa (c)).However, these factors can only assist in determining a breach, not describing details of the "appropriate or adequate investigation" that firms must undertake. Thus, the critical problem for this model is that most states do not stipulate an explicit method of investigation. In addition, there are no prescriptions for how a firm should document the results of an investigation. Some scholars have proposed that firms should be able to answer certain questions, such as where the stolen data were stored and how and by whom the data were accessed (Lesemann, 2010).

For a majority of state laws, the critical element for notification requirement is the resident of the victim, not the location of the firm or the breach. This could also be regarded as an increased burden on breached firms because they must comply with the requirements of state laws for each of their affected customers. Thus, breached firms could face multiple requirements if their victims are dispersed across the country.

Despite the varied scope and elements, the common factor of those state laws is a notification requirement that enables individuals to be aware of unauthorized access to their personal data. This leads to effects that will be discussed in the next section.

6.2 The impact of data breach notification laws

Data breach notification laws affect both firms and their customers. Firms may find that the notification requirement affects them positively and negatively. One potentially positive effect would be an improvement in a firm's data security practices. The main function of data breach laws, requiring business entities to notify upon discovery of a breach, is to "transform private information about firm practices into publicly-known information" (Schwartz & Janger, 2007). This function can create an incentive for business entities to take appropriate measures to protect personal data they collected. Notification could affect reputation because customers may lose confidence in breached firms (Ponemon, 2005). Apart from reputational damage, financial and economic aspects of the damage are evident. Notification can lower a breached firm's stock price, especially after a data breach caused by unauthorized access (Campbell et al., 2003).

Cavusoglu et al. (2004) demonstrated that notification can result in the loss of $2.1 of a firm's market valuation per stock. Acquisti et al. (2006) studied the effect of data breaches on stock market prices of such firms and found a "short-lived, reduction of 0.6 percent on the day that the breach is disclosed." Comparing breached and non-breached firms, Ko & Dorantes (2006) found that the sales and overall performance of breached firms is lower than that of non-breached firms. In addition, other costs are

associated with notification such as the cost of notifying costumers. Thus, firms appear to make security and operational investments in response to the disclosure requirement (Samuelson Law, Technology & Public Policy Clinic, 2007). Consequently, these effects can lead to a reduction of data breach events, thus deterring identity-related crimes.

Nevertheless, the notification requirement can also affect business entities negatively. First of all, it is argued that the cost and time spent regarding notification can be burdensome. As indicated above, data breach laws on the state level differ and are based on the residence of the individual victims. Thus, firms operating in multiple states must comply with the state laws of each of their affected customers. This can increase costs to breached firms.

Secondly, in some cases the potential for identity-related crimes may be low. Hence, it is argued that such notifications are an unnecessary cost for businesses. In addition, individuals may become desensitized if they receive too many notices (Cate, 2005).

Thirdly, some argue that the notification requirement can be an obstacle to the growth of e-commerce and technological development (Lenard & Rubin, 2006).

As for the impact on individuals, notification is regarded as a measure to ensure "the right to know" of individuals by informing them when their personal data are lost or stolen. The awareness can lead them to make decisions concerning the protection of their information from their perspective. Thus, individuals can take appropriate actions to prevent any identity-related crimes that may follow. For example, they can inform banks and other financial institutions to block transactions or to cancel accounts. In addition, they may change passwords and have credit cards reissued with new numbers. As a result, notification could increase consumer awareness of a data breach and encourage victims to be prepared for identity-related crimes that may follow.

Consequently, although there are some negative effects, data breach notification causes firms to take preventive measures to protect personal data. In addition, it causes individuals to be aware of the situation, thus allowing them to take preventive measures. This could lead to a reduction in identity-related crimes.

6.3 The comparative study of US and Thai laws

Regarding the preventive stage, i.e., the period before an identity-related crime has committed, several Thai laws relate to the protection of personal data, e.g., the Credit Information Business Act and the Official Information Act. Nevertheless, this paper indicates that these laws are insufficient and inappropriate as preventive approaches to identity-related crimes.

The "Official Information Act", B.E. 2540 (1997) could be regarded as a specific law related to the protection of personal information. This law's main purpose is to entitle an individual the right to access to public information controlled by a state agency, which is a constitutional right as appears in section 56 of the Thai Constitution B.E. 2550 (2007). Hence, provisions of this Act mainly involve the disclosure of public information (sections 7, 9, 11). However, this law provides an exception to the access of information in the case of "personal information". In addition, this Act indicates the principles of protecting personal information in section 23, such as the collection limitation principle, data quality principle, purpose specification principle and use limitation principle. Similar to U.S. data breach notification laws, the term "personal information" in this Act is broadly defined to include "information relating to all the personal particulars of a person, such as education, financial status, health records, criminal records or employment records, which contain the name of such person or contain a numeric reference, code or such other indications identifying that person as fingerprints, tapes or diskettes in which a person's sound is recorded, or photographed…" Compared with the US data breach notification, this Act has several limitations in applying to prevent identity-related crimes. Firstly, although there are several principles of personal data protection, there is no requirement for notification when there is unauthorized access to personal data. Secondly, the scope of this Act merely covers personal information in possession or control of a state agency. Thus, this Act excludes information in possession of private sectors such as financial and business firms.

Regarding the financial sector, Thai law specifically related to the protection of personal data is the Credit Information Business Act B.E. 2545 (second edition, B.E.2549).This law's objective is to protect the

right to know of financial institutions, which are granted the right to access credit information for analyzing the credit worthiness of clients. However, this law protects the right to privacy of individuals by stipulating data protection principles. According to the main principles of personal data, the "financial institutions" include commercial banks, finance companies, securities companies and insurance companies. They are required to submit client data to a "Credit Information Company", a firm that obtains a license to operate a credit information business that stores and processes the data. A financial institution that is a member of a credit information company is entitled to access personal information stored by the company.

The protection of data privacy consists of several principles as follows:

-Although a credit information company is required to disclose credit information to its members, which are financial firms, the disclosure can be done only under certain conditions set forth in section 20. The first condition reflects the "limitation of use" principle, i.e., the purpose of disclosure is allowed merely for analyzing the granting of credit and insurance. The second condition relates to the "consent" principle, i.e., a letter of consent from the owner of data should be obtained before disclosure. However, exceptions enable the disclosure without consent, such as a case whereby an order or summons is made by a court.

-The law excludes some sensitive data from being collected or stored, referred to as "prohibited information" (Section 3), and includes "physical handicaps, genetics, information of a person who is in the process of criminal proceedings."

-As for security in data processing, the law imposes a responsibility on credit information companies to prepare systems to protect the security of personal data, i.e., ways to secure the confidentiality and safety of information to prevent its abuse and to prevent unauthorized access to information, including systems to prevent information from being amended, damaged or destroyed illegally or without permission (Section 17).

Compared with U.S. data breach notification laws, this Act has several limitations that apply to preventing identity-related crimes. Firstly, the law's scope is limited merely to personal data of clients who apply for "credit", which includes, e.g., "a granting of loan or credit amount of loan, securities lending, hire-purchase, leasing". As a result, personal data possessed or stored by other business firms that are not engaged in a "credit" business fall out of the law's scope. Secondly, although it has several principles of personal data protection, including prevention of unauthorized access, this Act does not require financial firms to notify customers of an event of unauthorized access to their personal data.

Apart from these laws, in 2009 the Thai government adopted a draft of the Personal Data Protection Bill to protect information privacy. The bill aimed to protect personal information from being illegally used and disclosed without consent. A data controller was not allowed to transfer personal data to third countries having no data protection laws or having an inadequate level of protection without consent. The bill also would require businesses to develop preventive measures to protect personal information from being used without consent. However, the bill has not been enacted while it is in the process of revision by the Parliament. In addition, there is no "notification" principle in this draft bill.

Consequently, the lack of legal protection at the initial stage, i.e., when an unauthorized access of personal data or data loss occurs, exists in the current Thai legal environment. Individuals may even not know of a breach to their personal data in the possession of businesses. If there is a breach and a firm takes no action, it faces no legal liability. Thus, the risk of identity-related crimes is placed upon individuals who may or may not be victims. If an identity-related crime actually occurs, a second group of legal protections will be taken into consideration as proactive measures, which is beyond the scope of this paper.

7. Conclusion and Recommendation

A personal data breach can lead to identity-related crimes resulting in financial and reputational losses for both customers and business entities. From a legal perspective, there are two levels of protection. The first level involves laws that impose requirements on firms to notify individuals of unauthorized access to their personal information. These laws, referred to in the U.S.as "data breach notification or data breach disclosure", can be considered as a preventive approach to identity-related crimes. Nevertheless, Thailand's current legal system provides no specific laws regarding "data breach notification". Although Thailand has several laws related to the protection of personal data, e.g., the Credit Information Business Act and the

Official Information Act, these laws are insufficient and inappropriate as preventive approaches due to several limitations.

Consequently, this paper proposes solutions as follows:

- Regarding alternative measures, self-regulated notifications should be introduced by the commercial sector as a code of conduct regarding data security. In the absence of a legal requirement, this voluntary approach would increase consumer confidence and result in a positive impact on a firm's image and reputation.

- As for legal measures, this paper proposes that the Thai government enact specific laws incorporating the "data breach notification" principle by adopting U.S. state laws as a model to deter identity-related crimes. Since the U.S. data breach notification laws in the US consist of comprise two approaches with no clear details of "adequate investigation", this paper suggests a "strict liability" approach for Thai law. Therefore, notification should be required upon unauthorized access to personal data. This principle would be incorporated into the Credit Information Business Act B.E. 2545 (second edition, B.E.2549) by amendment to this Act. Alternately, this principle could be added to the draft bill of "the Personal Data Protection Bill" as part of its data protection principles.

8. References

Acquisti A., Friedman A., & Telang, R. (2006). Is there a cost to privacy breaches? An Event study. *Paper presented at the Fifth Workshop on the Economics of Information Security*, University of Cambridge, England.

Arango C., Hogg, D., & Lee, A. (2011).Why is Cash (Still) so entrenched? Results of the Bank of Canada 2009 Methods of Payment Survey. Discussion paper (forthcoming). Bank of Canada.

Arango, C., & Taylor, V. (2009). *The Role of Convenience and Risk in Consumers' Means of Payment*. Discussion Papers 09-8. Bank of Canada.

Barker, K.J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime 15*(4), 398-410.

Benton, M., Blair, K., Crowe, M., & Schuh, S. (2007). The Boston Fed study of consumer behavior and payment choice: a survey of Federal Reserve System employees. *Public Policy Discussion Paper 07-1*. Federal Reserve Bank of Boston.

Campbell, K., Gordon, L.A., Lobe, M.P, & Zhou L. (2003).The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of computer security, 11*, 431-448.

Cate, F. (2005). Another notice isn't answer. USA Today, Retrieved February 27, 2005, from http://www.usatoday.com/news/opinion/2005-02-27

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004).The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Cheney, J.S. (2010). Heartland Payment Systems: lessons learned from a data breach. *Payment Cards Center Discussion Paper 10-01*. Federal Reserve Bank of Philadelphia.

Commission - Joint Research Center, 2004.

Conkey, C. (2007). Assessing Identity-Theft Costs. *Wall Street Journal - Eastern Edition,*250.D3.

Crooks, T. (2004). Fear of ID Theft May Do More Harm than the Crime. *American Banker 169*(102), 10.

Europol (2006). *Organised Crime Threat Assessment*. Organisation For Economic Co-operation and Development. OECD Publishing: Paris.

Jonker, N. (2007). Payment instruments as perceived by consumers - Results from a household survey. *De Economist 155*(3), 271-303.

Jewkers, Y., & Yar, M. (2010). *Handbook of Internet Crime*. London: Willan Publishing.

Ko, M., & Doreantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of Information Technology Management, 17*(2), 13-22.

Koops, B. J., & Leenes, R.E.(2006). ID Theft, ID Fraud and/or ID-Related Crime - Definitions Matter. *Datenschutz und Datensicherheit 30*(9), 553-556.

Lenard, T., & Rubin, P.H. (2006). *Slow down on data security legislation*. Progress Snapshot 1.9. The Progress & Freedom Foundation.

Lesemann, D. (2010). Once More Unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes, *Akron Intellectual Property Journal, 4*, 203.

Listerman, R.A., & Romesberg, J. (2009). Creating a culture of security is key to stopping a data breach. Are we safe yet?, *Strategic Finance*, July, 27-33.

Mayer, R.N. (2009). Defending Your Financial Privacy: The Benefits and Limits of Self-Help. *AARP Public Policy Institute Issue Paper*. AARP Public Policy Institute.

McNally, Megan M. and Newman, Graeme, R. (2008). *Perspectives on Identity Theft.* New York: Criminal Justice Press.

Mitchison, N. et al. (2004). Identity Theft – A Discussion Paper, *Technical Report EUR 21098 EN*, European.

Organization for Economic Cooperation and Development (2008). OECD Policy Guidance on Online Identity Theft, Retrieve August 8, 2013, from http://www.oecd.org/dataoecd/49/39/40879136.pdf

Ponemon Institute (2005). *National Survey on Data Security Breach Notification*. The Ponemon Institute.

Samuelson Law, Technology & Public Policy Clinic. (2007). *Security breach notification laws: views from chief security officers*. University of California-Berkeley School of Law.

Schwartz, P., & Janger, E. (2007). Notification of data security breaches. *Michigan Law Review, 105*, 913-984.

Solove, D. J. (1997). Identity Theft, Privacy, and the Architecture of Vulnerability, *Hastings Law Journal, 5*(4), 12-28

Sproule, S. & Archer, N. (2010). Measuring identity theft and identity fraud. *Int J Bus Govern Ethics, 5*(1-2), 51-63.

Sullivan, R.J. (2008). Can Smart Cards Reduce Payments Fraud and Identity Theft? *Economic Review Federal Reserve Bank Kansas City, 93*(3), 35-62.

UK Cabinet Office (2002). *Identity Fraud: a Study*. London:UK Cabinet Office.

VISA (2011). *Payment Security*, Retrieved December 7, 2011, from http://www.visaeurope.com/en/about_us/what_we_do/payment_security.aspx