Data Breaches and Identity Theft: A Case Study of U.S. Retailers and Banking

Arika Artiningsih, A. Sudiana Sasmita

Abstrak

Pencurian identitas telah ada dan berlangsung cukup lama, sampai pada keberadaan internet yang makin meningkatkan jumlah dan fenomena kasusnya di seluruh dunia. Fenomena ini membutuhkan penanganan yang lebih baik dari segi system pengamanan data, teknik investigasi, produk hokum dan kolaborasi di level internasional. Penelitian ini bertujuan untuk mengungkap dan menganalisis secara mendalam kasus-kasus pembobolan database perusahaan secara *online* yang mengakibatkan terjadinya pencurian identitasdari para pelanggan. Mempertimbangkan cakupannya, penelitian ini membahas kasus pencurian identitas yang dicatatkan oleh dunia sebagai kasus dengan kerugian yang paling signifikan pada organisasi bisnis di Amerika Serikat, yaitu: *Target*, *JP Morgan*, *Home Depot*, dan *Sally Beauty*. Akan tetapi, mengingat sifat kasusnya yang melintasi batas-batas negara, maka penelitian ini melakukan analisis untuk membandingkan produk-produk hokum dalam mengatasi pencurian identitas *online* di beberapa Negara Eropa, Australia, dan ASEAN. Analisis Segitiga *fraud* digunakan untuk membongkar kasus-kasus pencurian identitas *online* dengan menyajikan jumlah korban dankerugian yang dideritasekaligusdampaktindakankejahataninikepada para pemangku kepentingan seperti investor, kreditor, bank, *credit union,* perusahaan, dan yang paling penting dampak terhadap pelanggan. Upaya penanganan hokum atas tindak kejahatan ini menarik untuk didiskusikan karena sifatnya yang melewati batas antarnegara. Pada gilirannya, tulisan ini memaparkan pentingnya pencegahan dan upaya bersama menangani tindak kejahatan inipada level organisasi, nasional maupun internasional.

Kata kunci: Kejahatan Online, PencurianIdentitas, Pembobolan Data, Peretas, Segitiga*Fraud*

Abstract

The objective of this paper is to evaluate the cases of online data breach and identity theft. According to Brodtmann (2011), identity theft has existed for long of time and the proportion has increased since the Internet has made the customer's personal information available online. This phenomenon has called better security, advance investigation techniques, law enforcement, and international collaboration. All the cases discussed would be limited for business organisations in the United States (U.S.), which are Target, JP Morgan, Home Depot and Sally Beauty. These cases are the most significant online identity theft recently occurred in the world. However, comparison of legislative reforms that addressed would be done for U.S., Europe, Australia and ASEAN due to the nature of the cybercrime that crossing the national boundaries. Fraud triangle would be use as the analysis tools. Victims and damages would be presented to show the consequences of this fraud to the stakeholders, including investors, creditors, community banks and credit union, the business itself and importantly the customers. Prosecution and legislative discussion would be provided to show how the governments over the world react to the issue of online data breach and identity theft that crossing national boundaries. Lastly but not least, recommendation to prevent and prosecute this kind of fraud would be given in the three levels, which are within the organisation, national level and international level.

Keyword: Cybercrime, Online Identity Theft, Online Data Breach, Hackers, Fraud Triangle

Introduction

First of all, identity theft has occurred "when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes" (Organization for Economic Co-operation and Development 2008, p.3). There are two ways to commit this act, online and offline (Jamieson et al. 2012, p.382). When identity theft has correlated with the misuse of computer, computer crime and computer-related crime because the Internet facilitate them, it called as online identity theft, for example is the case of hackers who stole someone's personal information through online data breach. In contrast, when the identity theft have committed through wallet theft, mail redirection and dumpster diving, it categorised as offline identity theft. This paperwould address the online identity theft caused by online data breaches in several business organisations, which are Target, JP Morgan, Home Depot and Sally Beauty. As cited in Roberds and Schreft (2009, p. 920), a data breach defined as an unauthorized access of personal data recorded by organization has promoted identity theft. Phishing, farming, malware and hacking are common methods that have been used to commit this action (Almerdas 2014, pp.84-6).

All the cases discussed have been limited for business organisations in the United States (U.S.). However, comparison of legislative reforms that addressed would be done for U.S., Europe, Australia and ASEAN due to the nature of the cybercrime that crossing the national boundaries. Moreover, these countries have been the main targets of cybercriminals. As evidence of this, even though there is no such case happened in Australia, the Attorney-General's Department reported that identity crime costs Australia up to $1.6 billion each year, with $900 million out of that number was contributed by individuals lost through identity theft, credit card fraud and scams (Australian Federal Police 2015).Then, looking to the U.S., the Ponemon Institute (2014) reports that the organization's cost for data breach and

identity theft is USD 3,900,000 while the damage for organisation's reputation and brand could be up to USD 330,000,000. The discussion would be started by the description of the cases, followed by the analysis, recommendation and conclusion.

Case Description

First of all, during the period of 2013-2014, U.S. have been shocked with several data breaches experienced by big retailers, which are: Target, Home Depot, Sally Beauty and one of the biggest banks, J.P. Morgan. It was the time when the nightmare of credit cards' holder have been started since their personal information and their financial information have been exposed, result in vulnerability that they might become the victims of identity fraud in the future.

Target data breach was the biggest identity theft in 2013. It was started in 27 November 2013 when the hacker put a malware named as RAM Scraper to its Point-of-Sales (PoS) terminal to copy the customer's personal information during the short moment when it was unencrypted and sent from PoS terminal to PoS register itself (Zorabedian 2014). This identity theft was occurred for two weeks before Target discovered it in 15 December 2015. This fraud has occurred because Target ignored the red flags given by its security team that spotted unusual activities in the payment system (Riley et al. 2014). Target's customers have not been informed yet until four days later when Target publicly admitted that their database has been compromised and 40 million customers' personal and financial information have been exposed, including names, credit card numbers, its expiration date, mailing addresses and emails. Later, in 10 January 2014, Target announced that additional 70 million customers' information has been stolen (Clark 2014). Target has missed its opportunities to prevent the data breach by ignoring the red flags given by its professional security team (Congressional Research Service (CRS) 2015, p.2-4).

Similar fraud has occurred for the Home Depot and Sally Beauty.

Hackers have infiltrated the Home Depot network and copy the customers' information from April 2014 to September 2014 when it was discovered. At that moment, 56 Million Credit Card payment details and 53 million customers' emails have been exposed. Meanwhile, in March 2014, Sally beauty also announced that 25,000 customers' records including payment card information has been exposed. The fraudsters of this breach were suspected from the same gang of Russian and Ukrainian hackers. As evidence of this, credit cards stolen from Sally beauty has been sold in Rescator[dot]cc, the same shop where the cards from Home Depot and Target have been sold. In addition, it was sold under batches named as "American Sanctions" and "European Sanction" which interpreted as a revenge for sanction given to Russia KrebsOnSecurity (2015).

The biggest identity theft recorded was J.P. Morgan. According to United States Securities and Exchange Commission Form 8-K (2014), J.P. Morgan reported lost of 76 million households and 7 million small businesses personal information including names, addresses, phone numbers, email addresses, and "internal JPMorgan Chase information relating to such users". The hackers were suspected from Russia also but different gang with the hackers that stole from Target, the Home Depot and Sally Beauty. As reported by Riley and Robertson (2014), the hackers have succeeded to enter the layers of sophisticated security system that seem far beyond the capability of ordinary criminal hackers. They added that FBI was involved in the investigation because of size of the loss and because the fraud has occurred when the tension between West and Russia increased. **Appendix A** provides summary of the cases in a table.

Research Methodology

The research method employed is called case study. This method allows the exploration and understanding of complex issues through reports of past studies. In addition, this method enable researcher to go beyond the quantitative method and understand the behavioral environments through

the actor's point of view (Zainal 2007, p.2). As a result, it could be used as a tool forreconstruction and analysis of the cases under investigation (Tellis,1997).

Therefore, firstly, this research conducted to what extent existing research has progressed towards clarifying a particular problem relating to data breaches and identity theft. Secondly,interrelation, contradictions, gaps and inconsistencies among cases were identified using fraud triangle analysis to figure out the reasons behind these fraudulent acts. Thirdly, the discussion would be extended to the point in which the world reacts to overcome this kind of fraud. Lastly,a recommendationwould provide to help the world prevent and overcome this problem.

Case Analysis

This section would analyse the cases described above using fraud triangle followed by the description about the number of victims and damages. Then, it would be ended with the discussion about prosecution and legislation discussion.

Fraud Triangle Analysis

Several factors behind the reason of the hackers to commit a data breach in order to steal the customers' personal information could be analysed using the elements of fraud triangle developed by Donald Cressey, which consists of perceived pressures, opportunities and rationalisation. Albrecht (2015) argued that anonymity of the hackers has made it difficult to discover the pressures and rationalisation. However, by using information combined from the investigations and previous studies we might be able to identify these elements.

As described before, several evidences indicated that the hackers were from Russia and. Blau (2004) argued that after the financial crisis in 1998, many people in Russia have lost their job, including professional such as computer programmers and business owners. The severe impacts are

persisting till today when the students who are excellent in algorithms and physics are difficult to find a job. Being a hacker offer them a solution to make money. Russia is as “a happy heaven” and “perfect breeding place” for hackers since people there are “overeducated and underemployment” (Blau 2004). This was proved when two hackers, 23 and 17 years old respectively, confessed that they were the creator of malware used to breach Target and Home Depot. The economics condition there might become worse after the U.S. and European economic sanction. As a result, we might conclude that the need of money for a living could be the main perceived pressure. Another pressure is greed since according to KrebsOnSecurity (2014), he hackers obtained 53.7 million by selling two million credit cards number of Target since each card was priced between18.00 and 35.7 dollar. Nevertheless, two million were only small amount of out of the total credit cards number that stolen. This amount was definitely easy money for the hackers. As Capers (2015) argued “identity is now a form of currency, and the consequences of this development are unfolding in interesting and often unpredictable ways”.

Perceived rationalisation would be the interesting element to discuss. A research conducted by Dremliuga (2014, pp.158-9) revealed that in Russia, hackers have been viewed as researchers instead of criminals because of the easy acceptance of hacker’s ideology. People in Russia believe that every single data should be for all humanity and the world of free computer information would be a better world. As a result, hackers believed that they were doing a good thing by helping people to provide free access to information. In addition Gostev, a security expert from Moscow-based Kaspersky cited in Blau (2004) stated that "I know of no hackers being imprisoned in Russia" and “They seem to be more interested in protecting national security". This makes people believe that hackers are not dangerous and then, even though Russia considers hacking as illegal and they have Russian Criminal code about criminal liability for illegal access (Article 272) and spreading of malicious software (Article 273), judge would choose soft penalty (Dremliuga 2014, p.160).

These were enough to rationalize that breaching a company's database to steal and then sell the customer's personal information were not something wrong. From their point of view, they have helped to create a better world with no information restriction. By doing this they might be proud and feel like a hero for Russia because the conflict between Russia and U.S. They might be not afraid to be caught also since they believed that their country would protect them in the same way as they protecting the national security. As an evidence for this, FBI investigation in J.P. Morgan case discovered a fact that no indication that the stolen information was used to benefit them financially (Masi 2014). Meanwhile, for the hacker gang that sold Target, the Home Depot and Beauty Sally credit cards' number for financial benefit, they might believe that they do not deceive the customers since they were only sold the cards that were used to steal the money. Lastly, they might believe that those organizations deserved for it since there were weaknesses in the security system implemented. From the hacker's point of view, the weaknesses of security system allowed them to enter and then it was not their faults if the customers' information was exposed.

Next, perceived opportunities came from the loopholes in security system that allow the hackers to break in the system. In addition, ignorance of the red flags and employees' security careless gave them opportunity to steal more. Kirk (2014) reported that hackers for Target and the Home Depot using the login credential from third party to enter their security system and it was suspected that they came from the same gang of hackers. For the Target data breach, the hackers were using credential login belonging from the heating and ventilation contractor, Fazio Mechanical Services and for the Home Depot, they used login credential from one of their vendors. When they entered to the system, they compromised the PoS system. These were slightly different with J.P. Morgan and Beauty Sally cases since in these cases they used credentials login from people within the company. In the J.P. Morgan case, the hackers used one of the employees'

user name and password to enter the web-development server that opened the way to the bank's main network (Goldstein et al. 2014). In addition, the bank has neglected to upgrade one of its network servers by not using two-factor authentication (Goldstein et al. 2014). Meanwhile, for Sally Beauty case, the hackers used a district manager's credential login. KrebsOnSecurity (2015) reported its interview with Blake Curlovic, an application support analyst of Sally Beauty who said, "This guy was not exactly security savvy. When we got his laptop back in, we saw that it had his username and password taped to the front of it".

In the Target case, ignoring the red flags has created more opportunity. At that moment, the Target has used FireEYe (FEYE), a professional security team used by Pentagon and CIA. FEYE has given an alert to Target when the spot the Malware in the PoS system in 30 November 2013 before the Hackers moved the data to the servers out of the country. However, Target ignored this alert (Riley et al. 2014). Lastly, because data breach and online identity theft were falling in the category of cybercrime, it was difficult to prosecute due to the national boundary protection. In these cases, the Hackers were in Russia that does not have extradition agreement with U.S. As a result, the U.S. law enforcements cannot catch and prosecute the hackers. In addition, the anonymity and lack physical contact would give the fraudsters more opportunity to commit the action since it was difficult to track their identities.

The summary of how they got opportunities and scheme used to enter the companies' system could bee seen in **Appendix B.**

Victims and Damages

The data breach consequences are not for the company only, but also for its stakeholders including investors, creditors, community banks and credit union. Equally important, the impact forcustomers.

In the last quarter of 2013 and the first quarter of 2014, after the data breach, Target's net income decreased up to 46% compared to the

previous quarter and its shares' price also declined by 9%. Similar financial losses also suffered by the Home Depot, Sally Beauty and J.P. Morgan. In addition, the companies might lose its reputation and customers' trust. Target has faced 90 lawsuits while the Home Depot has faced 44 lawsuits. The customers believe that that the companies should be able to do more in protecting their personal information.

For the employees, the decrease of revenue might result in permanent or temporary lay off. In the first quarter 2014, Target closed 133 stores in Canada, laid off 1,700 employees and 1,400 positions were unfilled due to the significant decrease of revenue (Bukaty 2015).The community banks also suffered losses since they need to reissue the credit cards. It cost them $200 million to reissue Target's customers credit cards and spent $90 million to reissue Home Depot's credit cards. Lastly, customers suffered the most since they might become the victim of identity fraud in the future. Once they become the victim of identity fraud, it would take so many effort, costs and time to get their identity and reputation back. For details and summary of financial losses caused by this data breaches, see **Appendix C.**

Prosecution and Legislative Discussion

The U.S. Assistant Attorney General Caldwell cited in The United States Department of Justice (DOJ) (2015) said "Cyber criminals conceal themselves in one country and steal information located in another country, impacting victims around the world" and "Hackers often take advantage of international borders and differences in legal systems, hoping to evade extradition to face justice". As a result, lacks of international collaboration in the form of extradition agreement and international treaty would challenge the investigation.

After more than a year investigation, no one has been charged for data breach in Target, Home Depot, Sally Beauty and J.P. Morgan. Anonymity, national boundary and the absence of extradition agreement between Russia and U.S. have made the investigation process getting

harder. RhinatShabayev (23) and Sergey Taraspov (17) have admitted that they were the creator of malware used in Target and The Home Depot (Selvan 2014). However, the U.S. could neither do further investigation nor prosecute them since they were living beyond the U.S. national boundary

The U.S. might be able to prosecute the hackers if they were living in a country that signed extradition agreement with the U.S. For an example, a Russian national, Vladimir Drinkman (34) who stole 160 million credit card numbers -the biggest data breach and identity theft that ever prosecuted in the U.S. after the prosecution of Albert Gonzales in 2010 for the same case- has been extradited to U.S. from Netherland where he was arrested (DOJ 2015). A recent case is the case of ArditFerizi(21) who had arrested in Malaysia in October 2015 and extradited to the U.S. for 20 years sentenced in January 2016 because he stole information (names, email, addresses, passwords, locations and phone numbers) for about 1,350 military personnel and federal staff and then sold itto ISIS as a hit list (BBC, 2016). DOJ as cited in BBC (2016) said that the case is the first kind and represented of "the nexus of the terror and cyber-threats". The latest case shows that identity theft and data breach is serious problem that could not only put someone's money in danger but also someone's life in danger.

Target and J.P. Morgan cases have triggered discussion in the U.S. about how to strengthen the national law in order to overcome the spurred of data breach that leads to online identity theft. As stated by CRS (2015, pp.19-23) the U.S. Congress has discussed about the need of federal notification requirement for data security breaches. Similar discussion also has been done in Europe and Australia. The different rules of Data Breach Notification Law in the U.S., Europe, and Australia and the proposal to improve it could be seen in the **Appendix D**.

In addition, the U.S. Congress also discussed the possibility of giving more authority to Federal Trade Commission's (FCT's) who has main responsibility to help the victims of identity theft to penalize business that fails to adequately protect the customers' personal information (CRS 2015,

pp.23-26). These reflect the need to strengthen the cybercrime related law to overcome the spurred of data breach that lead to identity theft.

Meanwhile, Australia has amendment its Commonwealth Criminal Code by enacting The Law and Justice Legislation Amendment Identity Crimes and Other Measures) Act 2010 (Cth) (Identity Crimes Act) on 2 March 2011 because they believe that the Commonwealth Criminal Code was not able to adequately facilitate the various form of identity theft due to the use of technology and internet that facilitate this action (Paphazy 2011, pp.28-9).

Then, in Europe, there is Europe's Convention on Cybercrime which also the only one of international treaty that addresses this issue. Other countries such as U.S., Canada, Japan, and Australia have signed this treaty also and U.S. has ratified it. (Jamieson et al. 2012, p.392).

Looking at another region, ASEAN which mostly consist of developed country has commitment to develop and adopt best practices and laws related to data protection in order to support and harmonize legal infrastructure for e-commerce in the Roadmap for Integration of e-ASEAN Sector (Chow and Redfearn2016). Singapore, Malaysia and Philippines had showed their commitment in data protection laws whereas Indonesia, Vietnam and Myanmar put data protection only in the part of electronic transaction law. Recently Indonesia has purposed a bill of data protection law. Chow and Redfearn (2016) also said thay if this bill is approved by the house of representative (Dewan Perwakilan Rakyat, DPR) then Indonesia need to reconcile this data protection law with the previous Act and government regulation related on it.

Recommendation

Recommendation would be given in the three levels, which are within the organisation, national level and international level.

First, within the organisation, the company should update and maintain their security system periodically to minimise the loops in the

system. Then, organisation policy should be made for both, prevention and detection of fraud. Security and fraud awareness training should be done to make the employees aware if there were suspicious activities in the system and keep them safe when using the Internet at home or at the office. Standard Operational Procedure (SOP) to follow up the alerts and red flags should be developed also. In the case of Target we might see that hiring the best professional security team was useless if there was no action to follow up the alerts. Segregation of duties should be created also between people who responsible for maintaining security system, servers and information assets. Lastly, organisation should consider the customer's information that they should and should not keep. Target has been criticised because they kept the credit card's PIN.

In the national level, the government should set a standard of minimum acceptable security system for business. In addition, penalties should be given for business organisation that fails to notify the customers without delay after the data breach. These are important for both, giving more protection to customers and preventing them to suffer more losses.

Lastly, because of the nature of cybercrime was crossing the national boundary, more international treaty and collaboration between country are needed since domestic law may be not able to go beyond the national boundary. The extradition of Vladimir Drinkman from Netherland to the U.S. has proved that collaboration was needed to prosecute the cyber criminals.

Conclusion

From the discussion above, current scheme to commit identity theft has been identified, which was through online data breaches. This was the easiest way to steal personal and financial information in a huge scale. In addition, it was preferable for the fraudster because they got anonymity and national boundary protection. Repercussion of action has happened for Home Depot,

Sally Beauty and J.P. Morgan after the hackers successfully breached and stole customers' information from Target.

These cases happened because the hackers have exploited the loopholes in organisation's security system. These could be in the form of out-dated security system such as in the case of J.P. Morgan that fail to implemented two-factors authentication, ignorance of alerts (red flags) such as in the case of Target or lack of security awareness trainings for employees and third parties that made them being the victims of social engineering by giving their credentials to the hackers.

Perceived pressures, rationalisations and opportunities of the hackers were similar because they came from the same country and then had similar background and motivation. The perceived pressures were the need for money and greed, the perceived opportunity were security system'sand internal control weaknesses as well as the ignorance of red flags. Lastly, the rationalisations were hackers' ideology and not deceiving the customers since they were only selling the cards used to steal the customers' money.

To overcome the spurred of this problem, organisation need to invest more in the security system as well as develop an organisation policy to support the security system. Fraud prevention and detection system such as an effective internal control system, fraud awareness training and whistle blowing mechanism are necessary to prevent these types of frauds from happening again in the future. Most importantly, business should invest more on the IT security system to protect their organisation from internal and external intruders, due to the heavy reliance of their process on the online systems.Last but not least, in the country level, international treaty and joint collaboration are needed to prosecute the fraudsters who hiding behind the national protection boundary. As a result, extradition agreement is absolutely needed to prosecute the hackers.

References

Albrecht, WS, Albrecht, CO, Albrecht, CC &Zimbelman, MF 2015, *Fraud Examination*, 5thedn,

Almerdas, S 2014, 'The criminalisation of identity theft under the Saudi Anti-Cybercrime Law 2007', *Journal of International Commercial Law and Technology*, vol. 9, no.2, Spring, pp.80-93, viewed 1 April 2015, LegalTrac database.

Anonym 2016, 'Hacker who aided IS sentenced to 20 years in US prison' BBC News, 23 September 2016, viewed 18 November 2016 <http://www.bbc.com/news/world-us-canada-37458168>.

Blau J 2004, 'Russia - a happy haven for hackers, Computer Weekly', *Computer Weekly*, 31 May, viewed 10 May 2015, <http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers>.

Bukaty, RF 2015, 'Target Offers $10 Million Settlement in Data Breach Lawsuit', The Two Way, 19 March, viewed 4 June 2015,<http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit>.

Capers, Z 2015, 'How We Innocently Give Away Our Data', *ACFE Insight,* 15 May, viewed 1 June 2015,<http://acfeinsights.squarespace.com/acfe-insights/2015/5/15/how-much-is-your-identityworth?mkt_tok=3RkMMJWWfF9wsRons6rPZKXonjHpfsX%2F4%2B4tXbHr08Yy0EZ5VunJEUWy2oAGRNQ%2FcOedCQkZHblFnVgJSq29RawNr6IE>.

Chow KW and Redfearn N 2016,'Data Protection in ASEAN' *Rouse the Magazine,* 4 July 2016, viewed 18 November 2016, <http://www.rouse.com/magazine/news/data-protection-in-asean/>

Clark M 2014, 'Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer', *International Business Time*, Viewed 12 May 2015 <http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056>.

Congressional Research Service 2015, 'The target and Other Financial Data Breaches: Frequently Asked Questions', CRS, viewed 27 May 2015, <https://www.fas.org/sgp/crs/misc/R43496.pdf>.

Dremliuga, R 2014, 'Subculture of Hackers in Russia', *Asian Social Science, Canadian Center of Science and Education,* vol. 10, no. 18, August, pp. 158-62, viewed 1 June 2015, DOAJ database.

Goldstein, M, Perlroth, N &Corkery, M 2014, 'Neglected Server Provided Entry for JPMorgan Hackers', *The New York Times,* 22 December, viewed online 6 June 2015, <http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/>.

Jamieson R, Land LPW, Winchester D, Stephens G, Steel A, Maurushat A, Sarre R 2012, 'Addressing Identity Crime in Crime Management Information Systems: Definitions, Classifications, and Empirics', *Computer Law & Security Review,* vol. 28, no.4, August,pp.381-95, viewed 4 April 2015, ScienceDirect database.

Kirk, J 2014, 'Home Depot says attackers stole a vendor's credentials to break in', PCWorld, 6 November, viewed 28 May 2015, <http://www.pcworld.com/article/2844832/home-depot-says-attackers-stole-a-vendors-credentials-to-break-in.html>.

Krebs, B 2015, 'Deconstructing the 2014 Sally Beauty Breach', *Krebs On Security blog*, web log post, 7 May, viewed 1 June 2015, <http://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/>

Krebs, B 2014, 'The Target Breach, By the Numbers', *Krebs On Security blog*, web log post, 6 May, viewed 17 May 2015, <http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/>.

Masi, A 2014, 'JP Morgan Chase Cyberattack: More Than 80 Million Accounts Compromised, Says New Report On Bank Hack', *International Business Time*s, 2 October, viewed 2 June 2015, <http://www.ibtimes.com/jp-morgan-chase-cyberattack-more-80-million-accounts-compromised-says-new-report-bank-hack-1698834>.

Organisation for Economic Co-Operation and Development 2008, *Scoping Paper on Online Identity Theft*, OECD Ministerial Meeting on The Future of Internet Economy, Seoul, viewed 1 June 2015,<http://www.oecd.org/sti/40644196.pdf>.

Paphazy, M 2011,'Online identity theft and the law', *Precedent*, no. 103, March-April, pp. 27-30, viewed 28 April 2015, APAFT database.

Ponemon Institute 2014, *Cost of Data Breach Study: Global Analysis,* viewed 18 November 2016, <https://www.935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf>.

Riley, MA, Elgin, B, Lawrence, D, &Matlack, C 2014, 'Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It', *Bloomberg*, 13 March, viewed 12 May 2015, <http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>.

Riley, MA & Robertson, J 2014, 'FBI said to Examine Whether Russia Tied to JPMorgan Hacking', *BloombergBusiness,* 28 August, viewed 1 June 2015, <http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking>.

Roberds, W &Schreft, SL 2009, 'Data breaches and identity theft', *Journal of Monetary Economics,* vol. 56, no. 7, October, pp. 918-29, viewed 28 May 2015, ScienceDirect database.

Selvan, S 2014, 'Russian Hacker RinatShabayev admits to be creator of BlackPOS Malware', *Ajay blog*, web log post , 22 January, viewed 4 June 2015, <http://www.radonit.in/ajay/category/blackpos-malware/>.

Smyth, S 2013, 'Does Australia Really Need Mandatory Data Breach Notification Laws – And If So, What Kind?**',** *Journal of Law, Information and Science,* vol. 22, no. 2, pp. 159-82,<http://www5.austlii.edu.au/cgibin/download.cgi/cgibin/download.cgi/download/au/journals/JlLawInfoSci/2013/8.pdf, AUSTLII database>.

Tellis, W 1997,'Introduction to Case Study',*The Qualitative Report*, Vol. 3, No.2, <http://www.nova.edu/ssss/QR/QR3-2/tellis1.html>

The Australian Federal Police (AFP) 2015, *About the Identity Crime*, AFP, Canberra, viewed 28 April 2009, <http://www.afp.gov.au/policing/fraud/identity-crime>.

The Department of Justice (DOJ) 2015, *Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States,* DOJ, Washington, viewed 6 June 2015, <http://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states>.

United States Securities and Exchange Commission (SEC) 2014, Form 8-K JP Morgan Chase & Co, SEC, Washington, viewed 3 June 2015, <https://www.documentcloud.org/documents/1308629->

Zainal, Z 2007,'Case Study as a Research Method',*JurnalKemanusiaan,* vol.9, <http://psyking.net/htmlobj-3837/case_study_as_a_research_method.pdf>

Zorabedian, J 2014, 'Target missed multiple warnings that credit card data breach was underway, *Naked Security*, 14 March, viewed 12 May 2015, <https://nakedsecurity.sophos.com/2014/03/14/target-missed-multiple-warnings-that-credit-card-data-breach-was-underway/>.

APPENDIXES

Appendix A Summary of the Cases

Descriptions	Target	Home Depot	Sally Beauty	J.P. Morgan
Time Lag fordiscovered	November 2013-January 2014	April 2014-September 2014	n.a. Discovered in March 2014	June 2014-October 2014
Number of Customers Impacted	110 Million	56 Million	25 Thousand	83 Million
Stolen Information	Names, account number, addresses, emails, PIN	Names, account number, card expiration date and a card verification value	Account numbers and security codes	Names, addresses, phone numbers, emails, and internal JPMorgan Chase information relating to such users

Appendix B. Methods to Exploit the Security System

Descriptions	Target	Home Depot	Sally Beauty	J.P. Morgan
Techniques used to enter the system	Stealing credential login of Heating and Ventilation Contractor	Stealing credential login of Vendor	Stealing District Manager's credential who careless with his user name and Password (tapped in his laptop)	Using Employee credentials that obtained through Phishing
System Compromised	PoS	PoS	PoS	90 servers of the banks
Type of Malware	RAM Scrapper/ BlackPOS	RAM Scrapper/ Mozart	RAM Scrapper/ FrameworkPOS and Timestomp	-

Appendix C Details and Summary of Companies' and Community Banks' Losses

Descriptions	Target	Home Depot	Sally Beauty	J.P.Morgan
Shares' Price	Decrease up to 9%	Not affected due to its strong market position	Decrease up to 1.41%	Decrease up to 3.5%
Investigation Expenses, offering customers' credit monitoring, opening more call centre	$17 Million reflected $61 million offset by $44 million insurance receivable. Additional $10 million to settle the data breach lawsuits	208 Million reflected $295 million offset by $90 million insurance receivable	n.a.	6.2 Billion
Cost to Upgrade Security system	$100 Million	n.a.	n.a.	$250 Million and 1000 people focused on security
Cost to Issue new credit cards by the community Bank	$200 Million to reissue 21.8 Million new Credit Cards	$90 Million to reissue 7.6 Million new Credit Card	n.a.	-

Appendix D Summary of the Data Breach Notification Laws in the U.S., Europe and Australia*

U.S.	Europe	Australia
Mandatory in 47 States Federal data breach notification law only mandatory for financial institutions, certain health care entities, and Health Information Technology	Mandatory for Electronic Communication Sector Two Condition: 1. Notify national authority (blanket duty to notify) if the data breach unlikely to give adverse impact for individual 2. Notify the individual without delay if the data breach likely to adversely impact personal information or privacy of the individual	Not a mandatory Prime Minister Julia Gillard's Government introduced a mandatory data breach notification bill into Parliament in May 2013
Congress discussed the policy to introduce comprehensive Federal Data Breach Notification Law for private sectors.	Propose to extend the obligations for companies in designated 'critical' sectors of the Europe	The Review of Australian Privacy Law recommended that a data breach notification scheme be implemented at the federal level

* The different of Data Breach Notification Law owned by U.S., Europe, and Australia. This table is generated based on the discussion from CRS (2015, pp.21-2) and Smyth (2013, pp.160-75)