They Did It For The Lulz: Future Policy Considerations In The Wake Of Lulz Security And Other Hacker Groups' Attacks On Stored Private Customer Data

By Jesse L. Noa*

"This is disgraceful and insecure: they were asking for it." - Lulz Security

I. INTRODUCTION

The prevalence of companies storing private customer data has risen dramatically since the advent of the internet.[1] This trend is illustrated by the fact that the amount of electronic data generated in 2011 was approximately 1.8 Zettabytes, or 1.8 trillion gigabytes.[2] Among the data being generated and stored by companies is customers' private information.[3] This data includes social security numbers, credit card information, account numbers, birth dates, addresses,

* Jesse Noa is a 2013 J.D. Candidate of Villanova University School of Law; He holds a B.A. in Economics, Aug. 2009, *summa cum laude*, Rowan University.

[1] *See* Stephen J. Rancourt, *Hacking, Theft, and Corporate Negligence: Making The Case for Mandatory Encryption of Personal Information*, 18 TEX. WESLEYAN L. REV. 183, 183-84 (2011) (noting dramatic increase in stored data and increasing importance for protective measures against theft).

[2] *See* John Gantz & David Reinsel, *Extracting Value from Chaos*, IDC IVIEW (June 2011), *available at* http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf (detailing growth of the 'digital universe').

[3] *See* Rancout, *supra* note 2, at 184-85 (discussing types of data typically stored by corporations).

emails, phone numbers, and other sensitive data that if misused, can destroy the finances of a person and potentially bring ruin to their lives.[4] Due to the increase of stored private data, protecting customer information is becoming increasingly important.[5] Failure to institute adequate protections for customer data has resulted in several classaction lawsuits due to security breaches by hackers.[6] These breaches have resulted in the loss of monumental amounts of customer data and the increased

---

[4] *See About Identity Theft*, FED. TRADE COMM'N (last visited Feb. 23, 2012), http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/about-identity-theft.html (discussing identity theft and its ramifications).

[5] *See id.* (estimating that each year over nine million Americans are victims of identity theft).

[6] *See e.g.*, Reilly v. Ceridian Corp., 664 F.3d 28, 40 (3d Cir. 2011) (suing for compromised data); Pisciotta v. Old Bat. Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (filing suit for lost customer data); Krotter v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010) (suing due to compromised customer data); Amburgy v. Express Scripts Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009) (filing suit as result of lost customer data); Hammond v. Bank of N.Y. Mellon Corp., No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307 *1-*2 (S.D.N.Y. June 25, 2010) (suing company due to customer data being compromised). One such hacker group was Lulz Security which was a loosely organized group of hackers who specialized in attacking poorly protected websites. *See Q&A: Lulz Security*, BBC NEWS AND TECHNOLOGY (last updated June 26, 2011, 4:30 p.m.), *available at* http://www.bbc.co.uk/news/technology-13671195 (answering various questions regarding hacker group Lulz Security). The group existed for fifty days before disbanding and during their time attacked a wide range of targets such as Sony and the Central Intelligence Agency. Recently, several arrests of the members of the LulzSec have occurred as a result of the help of one of the leaders who began working with the FBI. *See* Jana Winter, *EXCLUSIVE: Infamous International Hacking Group LulzSec Brought Down By Own Leader*, FOXNEWS (Mar. 02, 2012), http://www.foxnews.com/scitech/2012/03/06/hacking-group-lulzsec-swept-up-by-law-enforcement/ (detailing how LulzSec's leader helped FBI make major arrests through the organization).

possibility of identity theft.[7] This has been exemplified by the massive loss of private data by Sony at the hands of the hacker group Lulz Security and other hackers who exploited Sony's almost nonexistent network security.[8] Currently, companies have been shielded from liability for failure to protect the stored data through lackluster regulation on the state and federal levels as well as by burdens that plaintiffs must overcome in order to hold companies accountable in court.[9] Although this is the current state of affairs, the tides may be changing as new laws emerge which may expose companies to liability for their failings.[10]

This Comment explores the present state of private stored data, analyzing the current trends in the statutory and common law, and offers policy considerations for companies looking to avoid the explicit and implicit costs of a data breach. Part II outlines the significance of customer data protection in the digital age. Part III discusses the massive data breach at Sony, analyzing its legal and financial significance for corporate protection of customer data. Part IV provides an overview of other significant data breaches and their impacts. Part V examines the hurdles plaintiffs face when bringing claims against companies for inadequate data protection. Additionally, Part V discusses current state and federal laws, focusing on

[7] *See* Rancourt, *supra* note 1 at 185 (noting that Sony PlayStation network breach affected over seventy million customers and in TD Ameritrade's breach, over 6.3 million customers were affected).

[8] For a discussion regarding the Sony data breaches, see *infra* notes 25-91 and accompanying text.

[9] For a discussion regarding the legal burdens which plaintiffs have yet to overcome in brining data breach claims against companies, see *infra* notes 127-199 and accompanying text.

[10] For a discussion regarding the developing case and statutory law in the area of data breaches and company network security, see *infra* notes 127-199 and accompanying text.

their shortcomings. Finally, Part VI highlights several policy and financial considerations that companies should be mindful of in developing their network security and suggests guidelines companies should follow in the future.

II. THE CURRENT STATE OF PRIVATE STORED DATA

With the advent of the technological revolution, companies have increasingly used the internet as a means of conducting business.[11] As more commerce is conducted online, whether through direct sales, account memberships, online gaming, blogs, or other means, a staggering amount of customer data is being processed and stored on the internet.[12] As of 2011, the total amount of online stored data is estimated to be 295 exabytes, or 295 billion gigabytes.[13] To put this into perspective, on a single day American businesses generate more data than what "exist[s] in every book in every library in America."[14]

---

[11] *See* Timothy H. Madden, *Data Breach Class Action Litigation - A Tough Road for Plaintiffs*, 55 BOSTON B.J. 27, 27-28 (Fall 2011) (noting increased use of electronic methods of conducting business and greater need to transmit and store sensitive information).

[12] *See* Suzanne Wu, *How Much Information is There in the World?*, UNIV. SO. CAL. NEWS (Feb 10, 2011), *available at* http://uscnews.usc.edu/science_technology/how_much_information_is_there_in_the_world.html (discussing massive amount of information created and stored).

[13] *See* Lucas Mearian, *Scientists Calculate Total Data Stored to Date: 295+ Exabytes*, COMPUTERWORLD (Feb. 14, 2011), *available at* http://www.computerworld.com/s/article/9209158/Scientists_calculate_total_data_stored_to_date_295_exabytes (discussing recent study which calculated amount of data stored online).

[14] *See* Bennett B. Borden, *E-Discovery Alert, the Demise of Linear Review*, WILLIAMS MULLEN 1 (Oct. 2010), http://www.clearwellsystems.com/e-discovery-blog/wp-content/uploads/2010/12/E-Discovery_10-05-2010_Linear-Review_1.pdf (discussing amount of electronic data generated by American businesses in the course of one day).

As a result of the increased use of the internet as a means of commerce, consumers have had to adapt to a world where hackers can steal their identities, their banking and credit card information, as well as other types of personal data.[15] Hackers typically do this in order to steal money and make purchases under false identities, for activist reasons, or just for the fun of it.[16] Because of these risks, customers need to be assured that their personal data is protected.[17] Problems arise when companies storing personal data about their customers on online networks fail to enact appropriate security controls and procedures to ensure that the stored data is not compromised.[18] Due to the prevalence of the internet as a means for doing business, it is almost impossible for customers to avoid having their personal data stored by at least some companies.[19] When companies fail to adequately protect such data, customers become vulnerable to having their personal information used against them and are helpless to

---

[15] *See About Identity Theft*, *supra* note 4 (discussing types of information identity thieves steal and how they do so).

[16] *See id.* (noting hackers and thieves stealing identities to profit from victims). *See also* Kevin Komiega, *Political Hacking: Crime or Activism?* SEARCH SECURITY (Dec. 13, 2000), http://searchsecurity.techtarget.com/news/506135/Political-hacking-Crime-or-activism (discussing use of hacking and other electronic methods as form of political activism).

[17] *See* Fahmida Y. Rashid, *Fixing Data Breaches: Tracking the Cost and Damage Toll*, EWEEK (Mar. 14, 2011), http://mobile.eweek.com/c/a/Security/Fixing-Data-Breaches-Tracking-the-Cost-and-Damage-Toll-605411/ (noting increasing mistrust customers have regarding data breaches and customers leaving companies due to data breaches).

[18] For a discussion regarding the storage of data and the effects of a company not adequately protecting that data, see *infra* notes 119-126, 200-217 and accompanying text.

[19] *See* Madden *supra* note 12 at 27 (discussing increased use of e-commerce in day to day life).

prevent it, possibly to their financial detriment.[20] For example, in 2011 nearly twelve million Americans were victims of identity theft.[21] That same year, as a result of data breaches similar to the ones that occurred at Sony, the number of people whose personal information was stolen increased by sixty-seven percent.[22]

Companies who store their customers' data on online networks and databases should be considered to have taken on the duty to appropriately and adequately protect that data from theft and misuse.[23] Online attacks on company networks, facilitated by inadequate protection of customer data, can lead not only to potential legal liability but also to the alienation of customers, plummeting stock prices, loss of market share, and the financial ruin of customers whose identities have been stolen.[24]

---

[20] *See* FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers, FED. TRADE COMM'N (Sept. 3, 2003), *available at* http://www.ftc.gov/opa/2003/09/idtheft.shtm. (noting increase in identity theft and financial ramifications).

[21] *See* Mitch Lipka, *Rise in Identity Fraud Tied to Smartphone Use*, YAHOO FINANCE (Feb. 22, 2012), http://finance.yahoo.com/news/rise-identity-fraud-tied-smartphone-144531921.html (noting that amount of people affected by identity theft in America in 2011).

[22] *See id.* (discussing Sony's and other high profile data breaches' role in the increased proliferation of private customer data in the hands of hackers). For a discussion regarding the Sony and other data breaches, see *infra* notes 25-126 and accompanying text.

[23] For a discussion regarding companies storing customer data, the effects of not adequately protecting it, and policy considerations, see *infra* notes 25-126, 200-232 and accompanying text.

[24] For a discussion regarding the Sony data breaches and the effects on the company and its customers, see *infra* notes 25-91 and accompanying text.

III. THE "SOWNAGE CAMPAIGN": THE TOTAL DECIMATION OF SONY'S ONLINE NETWORKS

A. SOWNAGE: HOW HACKERS BROUGHT SONY TO ITS KNEES IN TWO MONTHS

Last year Sony was exposed for having inadequate network protection of their customer data through many uncoordinated attacks against both its PlayStation networks and its entertainment divisions.[25] The first attack was on April 04, 2011, by the activist hacker group Anonymous.[26] Anonymous attacked Sony's PlayStation Network ("PSN") with a Denial of Service attack ("DOS") in retaliation for Sony's lawsuit against George Hotz; better known in the online

[25] *See Absolute Sownage: A Concise History of Recent Sony Hacks*, ATTRITION (Last Updated June 4, 2011), http://attrition.org/security/rant/sony_aka_sownage.html (detailing hacks by various groups against all parts of Sony's business).

[26] *See id.* (detailing timeline of Sony's security breaches).

community as 'GeoHot'.[27] Although the DOS attack created a nuisance for Sony and its users, it did not compromise customer data. Following Anonymous'

[27] *See id.* (noting Anonymous declared war on Sony, attacking PlayStation Network in retaliation for Sony's lawsuit against GeoHot). The 'GeoHot' lawsuit involved Sony suing George Hotz for jailbreaking the Sony PlayStation 3 ("PS3"). *See* Audrey Watters, *Sony and "GeoHot" Settle PS3 Jailbreak Lawsuit*, READWRITEWEB (Apr 11, 2011), http://www.readwriteweb.com/archives/sony_and_geohot_settle_ps3_jailbreak_lawsuit.php (discussing Sony's settlement with George Hotz as well as details of lawsuit). Sony claimed that jailbreaking the PS3 allowed users to play pirated i.e., illegally obtained versions of the games on the PS3. *See id.* Sony also claimed that by jailbreaking the PS3, George Hotz breached the Digital Millennium Copyright Act as well as the Computer Fraud Abuse Act. *See id.* Jailbreaking involves hacking or modifying the game console in order to give the user access to the code of the gaming console. *See* Roydon Cerejo, *PS3 Jailbreaking: Is it Worth it?*, TECHTREE (Mar 28, 2011), http://www.techtree.com/India/Features/PS3_Jailbreaking_Is_it_Worth_it/551-114940-899.html (discussing what jailbreaking is as well as pros and cons for jailbreaking PS3). Anonymous "is not an organized collective of like-minded hackers. Rather, it's a banner that many different hacktivist groups rally behind in an attempt to gather enough support to take down an opponent." *See* David Goldman, *Hacker Group Anonymous a Nuisance, Not a Threat*, CNN MONEY (January 20, 2012), *available at* http://money.cnn.com/2012/01/20/technology/anonymous_hack/index.htm (detailing Anonymous as loosely affiliated activist hacker group). The actions of Anonymous are typically in the form of online protests to certain events such as the attack on Wall Street websites and systems in support of the Occupy Wall Street movement as well as attacks on the CIA, FBI, and entertainment websites in protest of the Stop Online Piracy Act ("SOPA"). *See id.* A DOS attack is where a hacker "attempts to prevent legitimate users from accessing information or services." *See* National Cyber Alert System, *Cyber Security Tip ST04-015: Understanding Denial-Of-Service Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM (Last Updated Nov. 4, 2009), *available at* http://www.us-cert.gov/cas/tips/ST04-015.html (detailing what DOS attack does to networks). Essentially, a DOS attack creates a flood of traffic to the target network, which overloads the servers, causing the network to go offline; preventing users' ability to access the network. *See id.*

attack on the PSN, a more substantial offensive was launched.[28]

On April 19, 2011, Sony became aware that the PSN was compromised and began investigating the source and effect of the breach but did not alert its users.[29] The next day on April 20, 2011, Sony took the PSN offline in response to the breach.[30] Despite this action, Sony did not publicly acknowledge that they knew of a data breach, but stated that, "[w]e're aware certain functions of the PlayStation Network are down. We will report back here as soon as we can with more information."[31] Additionally, Sony hired an outside security company to work on the PSN.[32] On April 21, 2011, Sony asserted that the PSN would be back online in a matter of days.[33] Further, Sony remained silent on the fact that PSN suffered a data breach even though numerous blogs and gaming news sites began questioning the possibility.[34] On April 22, 2011, Sony finally declared that an external breach was the cause of PSN being taken offline, stating, "[a]n external intrusion

---

[28] *See* Absolute Sownage, *supra* note 25 (detailing further hacks against Sony's network systems).

[29] *See* Martyn Williams, *PlayStation Network Hack Timeline: Major Events to Date in the PlayStation Network and Qriocity Hack*, NETWORK WORLD (Apr. 27, 2011), http://www.networkworld.com/news/2011/042711-playstation-network-hack.html (discussing timeline of PSN hack and Sony's response).

[30] *See id.* (noting Sony's choice to take PSN offline in response to data breach).

[31] *See id.* (discussing Sony's failure to inform public of data breach).

[32] *See id.* (noting Sony's decision to bring in outside security company to work on data breach investigation).

[33] *See id.* (observing that Sony claimed PSN would be back online within "a full day or two.").

[34] *See id.* (noting that several gaming related sources and blogs began reporting on possibility of a data breach being cause of PSN going offline).

on our system has affected our PlayStation Network and Qriocity services. In order to conduct a thorough investigation and to verify the smooth and secure operation of our network services going forward, we turned off PlayStation Network & Qriocity services."[35] Although Anonymous took responsibility for DOS attacks on the PSN in response to the GeoHot lawsuit, the group claimed that, as a whole, they were not responsible for the breach.[36] Additionally, Anonymous, as part of their denial of being the cause of the outage, hinted at the PSN security measures being fatally flawed.[37]

On April 23, 2011, Sony indirectly acknowledged the severity of the breach and inadequacy of its network security by stating that the PSN needed to remain offline to rebuild the entire system.[38] Sony gave no timeline of when they expected the PSN to be back

---

[35] *See id.* (discussing Sony's convoluted disclosure regarding external intrusion of PSN).

[36] *See id.* (noting that Anonymous claimed group was not responsible but that individual members may have acted against PSN.) *See also* Sara Yin, *'Anonymous' to Sony: For Once We Didn't do it*, PC MAGAZINE (Apr. 22, 2011), *available at* http://www.pcmag.com/article2/0,2817,2384012,00.asp (discussing Anonymous's denial that they caused PSN's outage).

[37] *See* Yin, *supra* note 36 (quoting Anonymous that Sony was attempting to blame PSN outage on Anonymous rather than fact PSN having internal problems). As part of their denial for the outage, Anonymous stated,

> [w]hile it could be the case that other Anons have acted by themselves AnonOps was not related to this incident and takes no responsibility for it. A more likely explanation is that Sony is taking advantage of Anonymous' previous ill-will towards the company to distract users from the fact the outage is actually an internal problem with the companies servers.

See id.

[38] *See* Williams, *supra* note 29 (discussing Sony's disclosure of fact that PSN network needed to be rebuilt as result of attack).

online.[39] On April 24, 2011, Sony hired a second outside security company to help work on the data breach, further highlighting the depth of the problem.[40] On April 25, 2011, although the outside security companies had concluded that the data breach resulted in customer data being compromised, Sony explicitly and publicly stated that such determination had not yet been made.[41] On April 26, 2011, the head of Sony's gaming division, Kaz Hirai, held a news conference in Tokyo and discussed the unveiling of the company's new tablet computers but did not discuss the PSN breach.[42] Later on that same day, Sony released a statement regarding the PSN breach.[43] At that point, Sony finally admitted that customer data was stolen as a result of the breach. Sony stated that:

> [W]e believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city,

[39] *See id.* (noting that there was no timeline of when PSN may be put back online).

[40] *See id.* (discussing Sony's hiring of second outside security company to work on PSN).

[41] *See id.* (noting security companies had discovered that customer data had been compromised as part of breach even though Sony publicly stated it was unsure if data had been breached and that Sony would notify consumers promptly if it was clear "personal information or credit card numbers of users had been compromised. . . .").

[42] *See id.* (discussing Mr. Hirai's decision not to take questions after conference and his failure to discuss PSN breach).

[43] *See id.* (noting that Sony gave its most detailed release regarding breach).

> state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained. If you have authorized a sub-account for your dependent, the same data with respect to your dependent may have been obtained. While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility. If you have provided your credit card data through PlayStation Network or Qriocity, out of an abundance of caution we are advising you that your credit card number (excluding security code) and expiration date may have been obtained.[44]

The number of users affected by the breach was approximately seventy-seven million.[45] The day after Sony made their public statement, a class action lawsuit was filed, alleging that Sony failed to take "reasonable care to protect, encrypt and secure the private and sensitive data of its users."[46] George Hotz responded to the breach on April 28, 2011, stating that, "[t]he fault

---

[44] *See* Patrick Seybold, *Update on PlayStation Network and Qriocity*, PLAYSTATION.BLOG (Apr. 26, 2011), http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/ (detailing official Sony statement regarding amount and type of data stolen as result of breach of PSN).

[45] *See Absolute Sownage*, *supra* note 25 (detailing number of users who had their data compromised).

[46] *See* Williams, *supra* note 29 (discussing pending class action lawsuit filed against Sony as result of inadequate network security and subsequent breach of PSN and Qriocity). Encryption is the use of sophisticated algorithms to convert the data into 'ciphertext' which cannot be easily understood without a key or the correct decryption technology, making it much more difficult to glean meaningful information unless having such tools. *See* Robert Bauchle, Fred Hazen, John Lund, Gabe Oakley, & Frank Rundatz, *Encryption*, SEARCH SECURITY (last updated July 2006), http://searchsecurity.techtarget.com/definition/encryption (defining encryption).

lies with the executives who declared a war on hackers, laughed at the idea of people penetrating the fortress that once was Sony, whined incessantly about piracy, and kept hiring more lawyers when they really needed to hire good security experts. . . ."[47] Additionally, a congressional committee contacted Sony asking them to explain and detail the massive data breach.[48] Finally, after being offline for twenty-five days, Sony reactivated the PSN.[49]

In addition to their problems with the PSN/Qriocity, other areas of Sony's business networks were being attacked.[50] On May 2, 2011, Sony shut down its Sony Online Entertainment Service ("SOES") after it was hacked.[51] As a result of the hack, Sony stated that it believed more than 23,000 customers' credit card and banking data may have been stolen.[52] It was also confirmed that hackers gained access to 24.6 million SOES users' personal information, similar to what was

---

[47] *See* Williams, *supra* note 29 (quoting George Hotz who claimed breach was in response to Sony's arrogance regarding network security and Sony's treatment of hacker and online community).

[48] *See id.* (noting U.S. congressional committee's contact with Sony).

[49] *See* Brandon Hill, *Sony PlayStation Network Comes Back Online*, DAILY TECH. (May 15, 2011), http://www.dailytech.com/Sony+PlayStation+Network+Comes+Back+Online/article21635.htm.

[50] *See Absolute Sownage*, *supra* note 25 (outlining numerous attacks on all aspects of Sony's business).

[51] *See* Robert McMillan, *Sony Cuts Off Sony Online Entertainment Service After Hack*, COMPUTERWORLD (May 2, 2011), *available at* http://www.computerworld.com/s/article/9216343/Sony_cuts_off_Sony_Online_Entertainment_service_after_hack (discussing Sony's decision to shutdown SOES after Sony discovered it was also hacked in addition to PSN). The SOES is a gaming network use for massive multiplayer online games ("MMOG"). *See id.*

[52] *See id.* (discussing data stolen as result of breach of SOES).

stolen through the attack on the PSN.[53] Additionally, as part of the hack on the SOES network, Sony stated that the hackers gained access to an outdated database which contained "card numbers and expiration dates for 12,700 customers based outside of the U.S., and direct withdrawal data belonging to some customers in Austria, Germany, the Netherlands and Spain."[54]

Sony's networks were again attacked on May 23, 2011, when the hacker group Lulz Security breached Sony Music Japan ("SMJ") through a simple Structured Query Language ("SQL") injection.[55] A SQL injection

[53] *See* Liana B. Backer & Jim Finkle , *Sony Hires Firm to Clean Up After Breach*, REUTERS (May 3, 2011), *available at* http://www.reuters.com/article/2011/05/03/us-sony-idUSTRE73R0Q320110503. (noting personal information such as names, email addresses, and passwords were also stolen as a result of SOES breach).

[54] *See* McMillan, *supra* note 51. (noting hackers ability to gain access to database with sensitive customer information).

[55] *See* Chester Winniewski, *Sony Music Japan Hacked Through SQL Injection Flaw*, NAKED SECURITY (May 24, 2011), http://nakedsecurity.sophos.com/2011/05/24/sony-music-japan-hacked-through-sql-injection-flaw/ (detailing Lulz Security's hack on SMJ and resulting compromise of customer data). For a discussion regarding Lulz Security, see *Q&A: Lulz Security*, *supra* note 5;

is a simple intrusion method that tricks a website and database into running codes that are not intended by the owner of the website/database.[56] Not only did Lulz Security breach SMJ, but they widely publicized the stolen information across the internet.[57] Luckily for customers of SMJ, Lulz Security was not a malevolent hacker group, but rather an activist group, and

---

A SQL injection attack is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database. Attackers take advantage of the fact that programmers often chain together SQL commands with user-provided parameters, and can therefore embed SQL commands inside these parameters. The result is that the attacker can execute arbitrary SQL queries and/or commands on the backend database server through the Web application. *See SQL Injection*, IMPERVA (last visited Jan. 31, 2013), http://www.imperva.com/resources/glossary/sql_injection.html (describing SQL injection attack). SQL has become very prevalent in web applications due to the use of databases to store and process information. *See SQL (Structured Query Language)*, NTC HOSTING (last visited Jan. 31, 2013), http://www.ntchosting.com/databases/structured-query-language.html (detailing SQL and its importance in maintaining and rationalizing information stored on online databases). "SQL is responsible for querying and editing information stored in a certain database management system." *Id.*

[56] *See* Steve Freidl, *SQL Injection Attacks by Example*, UNIXWIZ.NET (last modified Oct. 10, 2007), http://www.unixwiz.net/techtips/sql-injection.html (describing SQL injection and showing step by step application to take advantage of poor website security vulnerabilities). *See also*, Josh Shaul, *Why Do SQL Injection Attacks Continue to Succeed?*, SC MAGAZINE (May 24, 2011), *available at* http://www.scmagazine.com/why-do-sql-injection-attacks-continue-to-succeed/article/203679/ (noting ability to learn how to perform a SQL injection with little time and effort simply by searching "SQL injection how-to").

[57] *See* Winniewski, *supra* note 55 (discussing Lulz Security's publication of stolen user data from hack of SMJ).

accordingly did not publish sensitive data such as credit card or banking information.[58]

Sony's network problems continued as the Lebanese hacker known as "Idahc" breached Sony Ericsson through a SQL injection on the same day Lulz Security hacked SMJ.[59] The hack resulted in over 1,000 customers having their personal data compromised.[60] Similar to Lulz Security, Idahc published the stolen data online for anyone on the web to see.[61]

In response to these attacks, Sony should have changed its network protections or control systems or at the very least encrypted their customer data. Instead, on June 2, 2011, Lulz Security scored another massive breach on Sony Pictures, stealing over one million user logins as well as addresses and birthdates.[62] This time, Lulz Security did not hack for the 'lolz' but rather to teach a lesson, stating:

---

[58] *See id.* (noting Lulz Security did not publish banking or credit card information after hack of SMJ).

[59] *See* Thn Reporter, *Sony Ericsson Got Hacked by Idahc - Lebanese Hacker*, THE HACKER NEWS (May 24, 2011), http://thehackernews.com/2011/05/sony-erricson-got-hacked-by-idahca.html (detailing Idahc's breach of Sony Ericsson as well as posting links to hacked data).

[60] *See id.* (discussing amount and type of data compromised in Sony Ericsson hack). Sony Ericsson is a subsidiary of Sony which was recently renamed Sony Mobile Communications. *See* Jay Alabaster, *Sony Renames Ericsson Subsidiary Sony Mobile Communications*, COMPUTERWORLD UK (Feb. 16, 2012), http://www.computerworlduk.com/news/it-business/3337961/sony-renames-new-ericsson-subsidiary-sony-mobile-communications/.

[61] *See id.* (noting Idahc's publishing of compromised customer data).

[62] *See* Sam Biddle, *Hackers Spill Over 1,000,000 Sony Pictures Online Accounts*, GIZMODO (June 2, 2011), http://gizmodo.com/5807996/hackers-spill-over-1000000-sony-online-accounts (discussing Lulz Security's hack on Sony Pictures and subsequent release of customer data to the internet).

> [o]ur goal here [was] not to come across as master hackers, hence what we're about to reveal: SonyPictures.com was owned by a very simple SQL injection, one of the most primitive and common vulnerabilities, as we should all know by now. From a single injection, we accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?[63]

The hack by Lulz Security revealed that accessing the data was a simple matter, and showed that the customer data was stored in plain text rather than being encrypted, which rendered the information practically defenseless against malevolent hackers.[64] Lulz Security continued to attack Sony's networks and on the same day as the Sony Pictures hack, they breached Sony Bertelsmann Music Group ("BMG") and publicly posted Sony's developer source code as well as Sony BMG's network maps.[65]

---

[63] *See id.* (noting Lulz Security's explanation for hacking and releasing Sony Pictures customer data) (emphasis in original).

[64] *See id.* (discussing Sony's complete failure to protect their customers' data from hackers).

[65] *See* Diane Bartz, *LulzSec Hackers Claim ANOTHER Sony Hack, Post Alleged Source Code Online*, HUFFINGTON POST (June 6, 2011), *available at* http://www.huffingtonpost.com/2011/06/06/lulzsec-hackers-sony-bmg-network-maps_n_872187.html (detailing Lulz Security's hack on Sony BMG). Source code "refers to the programming language one uses to write a program." *See What is Source Code?* WISEGEEK (last visited Mar. 3, 2012), http://www.wisegeek.com/what-is-source-code.htm (describing source code and its functions). A network map is "graphical representation of all the computers and devices on your network that shows how each is connected." *See Network Map*, WEBOPEDIA (last visited Mar. 11, 2012), http://www.webopedia.com/TERM/N/network_map.html.

Sony's problems continued on June 20, 2011, when hackers Idahc and Auth3ntiq gained access to 177,000 emails from Sony Pictures France.[66] Yet again, one of Sony's networks was breached through a simple SQL injection.[67] Fortunately for the users of Sony Pictures France, the hacking duo did not publish their user information on the internet.[68] According to Idahc, he breached Sony Pictures France to prompt Sony to improve their security.[69] With the addition to Idahc and Auth3ntiq's hack on Sony Pictures France, the number of successful breaches of Sony's networks reached twenty in a matter of two months.[70]

The sheer number of successful breaches of Sony's networks showed that despite taking several of its networks offline in response to the initial security breaches, Sony had failed to fix the fundamental security

---

[66] *See* Erica Ogg, *Hackers Claim 177k E-mails From Sony Pictures France*, CNET (June 20, 2011), http://news.cnet.com/8301-31021_3-20072668-260/hackers-claim-177k-e-mails-from-sony-pictures-france/?tag=txt;title (discussing Idahc and Auth3ntiq's hack on Sony Pictures France).

[67] *See id.* (discussing method used to hack into Sony Pictures France). The SQL injection method had been used previously as discussed above to steal user information from Sony Music Entertainment Japan, SonyPictures.com and Sony Pictures Russia. *See id.*

[68] *See id.* (noting that hackers did not publicly publish compromised user data).

[69] *See id.* (discussing Idahc's interview with Forbes Magazine in which Idahc claimed the hack was for purpose of motivating Sony to improve its network security).

[70] *See id.* (noting number of recent hacks of Sony's networks after initial PSN data breach).

problems of its networks.[71] Furthermore, the success of these attacks demonstrated Sony's complete failure to adequately secure their networks in the first place.[72] These attacks drew attention to the corporation's ignorance, apathy, or arrogance in not properly protecting the customer data stored on their networks.[73]

The widespread significance of the attacks on Sony's network is underscored not only by the company's potential legal liability, but various other negative consequences Sony experiences due to their failure to adequately protect their customers' data. The breach caused severe alienation among Sony's customer base and created a lack of trust in what was once a pristine name brand corporation.[74] This lack of trust can result in a massive loss in market share for Sony and

---

[71] *See* Kevin Fogarty, Latest Hack Shows Sony Didn't Plug Holes: LulzSec Thanks for Revealing Sony Hypocrisy; Now Can You Stop Punishing Its Customers?, PC WORLD (June 5, 2011), *available at* http://www.pcworld.com/article/229421/latest_hack_shows_sony_didnt_plug_holes.html (discussing Sony's clear failure to address fundamental, enterprise wide problems which resulted in and still continue to exhibit security flaws in Sony's networks) (last visited, January 15, 2013).

[72] *See Absolute Sownage*, *supra* note 25 (noting the preposterousness of even debating whether attacks on Sony were advanced, stating that Sony failed to "implement[] what any rational administrator or security profession would consider 'the basics.' Storing millions of customer's personal details and passwords without using any form of encryption is reckless and ridiculous.").

[73] *See id.* (discussing the reckless lack of security of Sony's data networks).

[74] *See* Winda Benedetti, *Sony Sued, Could Bleed Billions Following PlayStation Network Hack*, MSNBC (Apr. 27, 2011), *available at* http://ingame.msnbc.msn.com/_news/2011/04/27/6544610-sony-sued-could-bleed-billions-following-playstation-network-hack (discussing international outrage and lack of trust in Sony as a result of the PSN hack and Sony's response as well as lack of security of its networks).

companies like it.[75] Further, such disregard to protecting customer data can lead to substantial losses in company value and drop in stock prices.[76] These results are important for any company storing customer data to consider when deciding on policies and procedures for protecting such data.

B. SETTING SAIL FOR FAIL: HOW SONY'S INADEQUATE NETWORK SECURITY INVITED THE SOWNAGE CAMPAIGN

Where did Sony go wrong? Why was Sony targeted and attacked so many times? The answers lie in the statements of Lulz Security and Idahc who attacked Sony's networks: it was done not only for the fun of it, but to show the public that a major corporation which was supposed to keep customer data private and protected, essentially left the door open to anyone who wanted to steal the information.[77]

---

[75] *See* Rashid, *supra* note 17 (discussing large costs associated with data breaches and how it drives costumers away from companies).

[76] *See* Eric W. Dolan, *Sony Loses 3.2 Billion After PlayStation Network Hacked*, RAW REPLAY (May 3, 2011), http://www.rawstory.com/rawreplay/2011/05/sony-loses-3-2-billion-after-playstation-network-hacked/ (discussing Sony's posting a 3.2 billion dollar loss after breach of PSN). *See also* Steven Williamson, *PlayStation Network Hack Causes Drop in Sony Share Prices*, PLAYSTATION UNIVERSE (Apr. 28, 2011), http://www.psu.com/PlayStation-Network-hack-causes-drop-in-Sony-share-prices--a011485-p0.php (detailing eight percent drop in Sony's share price as a result of hack of PSN).

[77] *See* Julianne Pepiton, *Group Claims Fresh Hacks of 1 Million Sony Accounts*, CNN MONEY (June 2, 2011), http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/index.htm (noting that Lulz Security stated "Sony was 'asking for it' by storing more than 1 million user passwords in plain text, instead of encrypting them."). Lulz Security also stated that the level of security maintained by Sony was "disgraceful." *See id.*

Sony's major mistake was having little to no security for its stored data in the first place.[78] Simple SQL injections should not be able to affect the databases of multi-billion dollar corporations and could have been avoided with simple security procedures.[79] Furthermore, Sony failed to encrypt its users' data.[80] It could be argued that such encryption is unnecessary for easily accessible public information, but birthdates, account information, credit card numbers, and other financially sensitive information should be encrypted in order to protect against potentially devastating fraud and identity theft.[81]

Another glaring issue regarding the data breaches was how Sony addressed it with the public.[82] Sony waited one week after the discovery of the breach to notify its customers that their data had been

---

[78] *See Absolute Sownage*, *supra* note 25 (noting that "Sony has demonstrated they have not implemented what any rational administrator or security professional would consider 'the absolute basics.'").

[79] *See* Shaul, *supra* note 56 (discussing ease for hackers to use SQL injection attack and lack of difficulty to protect against such attacks with simple security procedures and vigilance).

[80] *See* Peter Cohen, *Sony Encrypted Credit Card Data, but not User Account Info*, ZDNET (Apr. 28, 2011), http://www.zdnet.com/blog/gamification/sony-encrypted-credit-card-data-but-not-user-account-info/344 (noting Sony failed to encrypt users' account information on PSN).

[81] *See id.* (noting that even though Sony encrypted credit card information, Sony failed to disclose what type of encryption was used and if it was adequate). Why Sony did not encrypt the user account information has been the topic of expert and political discussions since the breach. *See id.*

[82] *See* Davey Winder, *Where Hacked Sony Went Wrong, and LastPass Got it Right*, PCPRO (May 6, 2011), http://www.pcpro.co.uk/blogs/2011/05/06/where-hacked-sony-went-wrong-and-lastpass-got-it-right/ (discussing Sony's response to the data breaches).

compromised.[83] In the fast-paced computing world, such a slow response is unacceptable and reckless.[84] Hackers had a week to launch any fraud or identity theft campaigns they wanted without Sony's customers having any warning or ability to take the appropriate actions to protect themselves.[85] As one of the largest entertainment companies in the world, such a delayed response is unacceptable not only from a customer standpoint but from a financial and managerial point of view.[86]

Sony's failings not only put their customers at risk but also created severe financial ramifications for the company.[87] For example, the PSN was taken offline for twenty-five days, which prevented users from playing online, purchasing games, movies, or other services from Sony.[88] The outage was estimated to cost Sony ten million dollars per week.[89] The total estimated

---

[83] *See id.* (discussing Sony's delayed response in notifying its customer base of data breach).

[84] *See id.* (noting how exposed customers became within one week).

[85] *See id.* (detailing customers inability to take steps to protect themselves due to lack of notice).

[86] *See id.* (implying that company of Sony's size should have responded quicker to the issue and claiming such response was "[s]imply not good enough").

[87] For a discussion regarding the potential financial ramifications of a data breach, see *infra* notes 119-126, 200-217 and accompanying text.

[88] *See* Hill, *supra* note 50 (discussing PSN coming back online). The PSN allows users to play online with other PlayStation users, as well as rent or buy movies, video games, and other services. *See PlayStation®3 Features*, PLAYSTATION (last visited Mar. 11, 2012), http://us.playstation.com/ps3/features/ps3featuresnetwork.html (describing features of PlayStation and PSN).

[89] *See* Alex, Pham, *PlayStation Network Security Breach Will Cost Sony Much More Than Money*, L.A. TIMES (Apr. 28, 2011), *available at* http://articles.latimes.com/2011/apr/28/business/la-fi-0428-ct-sony-hack-20110428 (noting that PSN outage cost estimated ten million dollars per week).

cost of the breach as well as the steps Sony took to remedy it was approximately $171 million.[90] Furthermore, Sony's actions breached its customers' trust which may prevent future sales as well as drive customers to competitors.[91] These negative consequences can be felt by any company that fails to institute adequate safeguards for consumer data stored online.

IV. OTHER NOTABLE DATA BREACHES

Sony was not the only company in recent years to have their databases breached by hackers.[92] Many large companies, particularly in the finance industry, have been the focus of hacker attacks.[93] Below is a short description of data breaches that have occurred at some major companies over the past few years, which further demonstrates the significant impact inadequate data protection can have on corporations and consumers.

---

[90] *See* Mathew J. Schartz, *Sony Data Breach Cleanup to Cost $171 Million*, INFORMATION WEEK (May 23, 2011), *available at* http://www.informationweek.com/news/security/attacks/229625379 (discussing costs incurred by Sony due to data breaches against Sony's networks).

[91] *See* Pharm, *supra* note 89 (noting PSN customer who stated "I doubt I will ever put my credit card information on their network again.").

[92] *See* Fahmid Y. Rashid, *IT Security & Network Security New & Reviews: 10 Biggest Data Breaches of 2011 So Far*, EWEEK (May 25, 2011), http://www.eweek.com/c/a/Security/10-Biggest-Data-Breaches-of-2011-So-Far-175567/ (discussing numerous major data breaches at major companies such as Sony, Epsilon Alliance Data Systems, WordPress, University of South Carolina, and Expedia).

[93] *See* Victoria McGrane & Randall Smith, *Hacking at Citi is Latest Data Scare*, WALL STREET JOURNAL (June 9, 2011), *available at* http://online.wsj.com/article/SB10001424052702304778304576375911873193624.html (noting that security experts claim financial institutions are "top target[s] for cybercriminals"). The security experts further noted that "[t]he most sophisticated hackers in the world target banks, and they target government agencies. . . ." *See id.*

A. CITIGROUP

In June of 2011, Citigroup was the focus of a major data breach that resulted in the compromise of over 360,000 customers' data.[94] The stolen information included names, addresses and account numbers.[95] Citigroup's response was to inform their customers within two weeks of discovering the breach and replacing the majority of their affected customers' credit cards.[96] Unlike the Sony breaches, the breach at Citigroup was the result of sophisticated hacking methods which involved an automated tool that repeatedly typed account numbers into the browser address bar in order to access the information.[97]

B. RSA SECURITY

In March of 2011, alarms around the world went off when the premier computer security company, RSA Security ("RSA"), was hacked.[98] This data breach was of significant importance because of the widely held view that if RSA could be hacked, then any company could be.[99] The information stolen involved RSA's SecurID products which provide additional protection to

---

[94] *See* Kim Zetter, *Citi Credit Card Hack Bigger Than Originally Disclosed*, WIRED (June 16, 2011), *available at* http://www.wired.com/threatlevel/2011/06/citibank-hacked/ (discussing disclosure of increased number of accounts which had been compromised at Citigroup, bringing number from 200,000 to 360,000).

[95] *See* McGrane, *supra* note 93 (detailing type of data stolen in hack of Citigroup).

[96] *See id.* (discussing Citigroup's response to the data breach).

[97] *See* Zetter, *supra* note 94 (discussing method used by hackers to gain access to Citigroup's customer account data).

[98] *See* Kim Zetter, *Hacker Spies Hit Security Firm RSA*, WIRED (Mar. 17, 2011), *available at* http://www.wired.com/threatlevel/2011/03/rsa-hacked/ (detailing security breach at world's premier computer security firm).

[99] *See* McGrane, *supra* note 93 (noting that "RSA 'is like Fort Knox. If RSA can get hacked, anybody can get hacked.'").

the user login process by "requiring users to enter a secret code number displayed on a key fob, or in software, in addition to their password."[100] This is important because over 250 million RSA customers use SecurID, which could potentially expose them to hacker attacks.[101]

Unlike the instances at Sony, which practically left the virtual door open, the hack at RSA involved a sophisticated three stage attack.[102] The first stage involved sending phishing emails to small groups of employees, one of whom opened the email which contained malware.[103] The malware exploited "a previously unknown flaw in Adobe's Flash software

---

[100] *See* Zetter, *supra* note 98 (detailing type of data stolen and what SecurID involves). SecurID is a two-factor authentication technology which creates an extra layer of protection over a simple password login. *See id.*

[101] *See id.* (discussing effect breach of RSA may have on customers who use SecurID technology).

[102] *See* Riva Richmond, *The RSA Hack: How They Did it*, N.Y. TIMES (April 2, 2011), *available at* http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/ (detailing how sophisticated attack on RSA was accomplished). *See also Absolute Sownage*, *supra* note 25 (noting "the attacks on Sony are not coordinated, nor are they advanced.").

[103] *See* Richmond, *supra* note 102 (discussing initial step hacker used to gain access to RSA system). The initial attack was successful when a single employee took the email out of the spam folder and opened the attached excel file. *See id.* Phishing "is a fraudulent attempt, usually made through email, to steal [someone's] personal information. . . . Phishing emails usually appear to come from a well-known organization and ask for your personal information—such as credit card number, social security number, account number or password." *See What is Phishing*, PHISHTANK (last visited Feb. 16, 2012), http://www.phishtank.com/what_is_phishing.php (defining phishing scam). Scammers will use emails with legitimate sounding titles and themes to try and coax potential victims into giving them their personal information. *See id.* The scammers later use that information to steal the victim's identity and money. *See id.*

[allowing it] to install a backdoor."[104] With the backdoor in place, the hacker was able to steal passwords of that employee, enabling the hacker to gain access to other systems and other employees.[105] After gaining access to the target files, the hacker sent the data to "a hacked machine at a hosting provider, and then on to the hacker himself."[106]

C. LOCKHEED MARTIN

The far reaching implications of the RSA security breach were seen when the information stolen from RSA was later used to gain access to the data of Lockheed Martin ("Lockheed") at its main database center in Maryland.[107] Hackers used "falsified SecurID electronic tokens to gain access" to Lockheed's databases.[108] Fortunately, Lockheed had broader

---

[104] *See id.* (explaining how malware was able to give hacker control over RSA employee's computer). A backdoor program "allows the hacker to access [a] computer whenever it's on the [i]nternet. It's a remote control, and usually a very thorough one with full access to every facility and file on [a] computer." *See What Hackers Do*, TINHAT (last visited Mar. 11, 2012), http://www.tinhat.com/hackers/hacking.html.

[105] *See* Richmond, *supra* note 102 (detailing how hacker was able to use employee's computer and passwords to gain access to other parts of RSA, enabling hacker to gain access to sensitive data).

[106] *See id.* (describing how hacker was able to transmit stolen data from RSA to controlled computer). The hacker left very few clues behind other than three Web addresses, one of which indicated a possible connection with the People's Republic of China. *See id.*

[107] *See* Jason Mick, *Reports: Hackers Use Stolen RSA Information to Hack Lockheed Martin*, DAILY TECH (May 30, 2011), http://www.dailytech.com/Reports+Hackers+Use+Stolen+RSA+Information+to+Hack+Lockheed+Martin/article21757.htm (detailing hack and loss of highly sensitive data from Lockheed Martin's massive data center in Maryland).

[108] *See* Kwame Opam, *Lockheed Martin's Security Networks*, GIZMODO (May 28, 2011), http://gizmodo.com/5806485/lockheed-martins-security-networks-were-hacked (noting how hackers were able to gain access to Lockheed's networks).

security systems which were able to lessen the effectiveness of the hackers' attack.[109] Accordingly, Lockheed was able to quickly discover the attack and minimize the areas affected by the breach.[110] As a result of its quick actions, Lockheed stated that there was "no compromise of customer, program or employees' personal data. . . ."[111] Although Lockheed claimed that no sensitive data was compromised, the very fact that hackers may have been able to gain access to classified United States military research and defense files underscores the stakes involved with protecting stored data.[112]

D. BANK OF AMERICA

The financial costs of a data breach were illustrated when Bank of America suffered a data breach which allowed hackers to steal "at least $10 million from the bank."[113] This breach was not the result of a highly sophisticated hack, as was the case in the RSA breach, but rather by a low tech method; an insider leaked

---

[109] *See id.* (stating that Lockheed's broader security measures helped "soften the blow" from the breach).

[110] *See* Mick, *supra* note 107 (noting that Lockheed "detected the [hack] 'almost immediately' and warded it off quickly.").

[111] *See id.* (noting Lockheed's claim that breach on their network did not compromise secured data).

[112] *See id.* (detailing some of stored data as relating to "the F-16, F-22 and F-35 fighter aircraft; the Aegis naval combat system; and the THAAD missile defense.").

[113] *See Insider Data Breach Costs Bank of America Over $10 Million, Says, Secret Service*, INFO SECURITY (May 26, 2011), http://www.infosecurity-magazine.com/view/18237/insider-data-breach-costs-bank-of-america-over-10-million-says-secret-service/ (discussing financial impact data breach had on Bank of America).

confidential information to scammers and hackers.[114] The information leaked included names, addresses, social security numbers, bank account numbers, birthdates, drivers' licenses, and more.[115] This information gave the scammers the ability to fraudulently withdraw money from the customers of Bank of America.[116] The ability for an employee to steal and leak customer information so easily shows a flaw in Bank of America's data protection policy. This was especially apparent because Bank of America had stated it was going to strengthen its data security due to threats from Wikileaks regarding the release of "damaging

---

[114] *See* David Lazarus, *Bank Of American Data Leak Destroys Trust*, LA TIMES (May 24, 2011), *available at* http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524 (detailing how customer data was leaked to scammers by former employee). The leaked data was later used to fraudulently withdraw funds from customer accounts. *See id.* Bank of America is not the only company to lose the sensitive data of their customers through very low-tech means. British Petroleum ("BP") recently lost the personal data of over 13,000 people who had filed claims against BP as a result of the Gulf oil spill simply because a BP employee lost the laptop containing the information. *See* Associated Press, *BP Loses Laptop With Gulf Residents' Claim Data*, CBS NEWS (Mar. 29, 2011), http://www.cbsnews.com/stories/2011/03/29/business/main20048504.shtml.

[115] *See* Lazarus, *supra* note 115 (listing type of customer data leaked to scammers).

[116] *See id.* (discussing how hackers were able to withdraw money from customer accounts using Andrew Goldstein, Bank of America Customer, as example). Not only were the scammers able to use the stolen data to get checks, but they also contacted Bank of America's customer service to successful transfer funds from non-compromised accounts to compromised ones. *See id.*

information."[117] As a result of the leak, Bank of America has had to reimburse its customers who had their money stolen as well as provide two years of free credit monitoring, all of which goes towards the estimated ten million dollars the bank lost.[118]

E. NORTEL

The pervasiveness of a data breach was illustrated in the hack of Nortel.[119] It was recently discovered that hackers had unimpeded access to Nortel's corporate computer system for over ten years.[120] Hackers were able to steal the passwords of key executives and as such, "had access to everything."[121] As with other data breaches, the hackers were able to gain access to sensitive information such as "technical papers, research-and-development reports, business plans, employee emails and other documents."[122] The disturbing factor regarding the breach was Nortel's

---

[117] *See id.* (noting that Bank of America claimed it would "enhance" its data security as a result of the threat yet the scammers were still able to fraudulently access customer accounts). Wikileaks is a whistle-blowing website which has released thousands of classified documents, typically from governments or large corporations, on the internet. *See* Jonathan Fildes, *What is Wikileaks?*, BBC NEWS AND TECH. (Dec. 7, 2010), *available at* http://www.bbc.co.uk/news/technology-10757263.

[118] *See* Lazarus, *supra* note 114 (discussing Bank of America's response to data breach and loss of customer trust).

[119] *See* Jameson Berkow, *Nortel Computers Breached by Hackers for Over a Decade: WSJ*, FINANCIAL POST TECH. DESK (Feb. 14, 2012), *available at* http://business.financialpost.com/2012/02/14/nortel-computers-breached-by-hackers-for-over-a-decade-wsj/ (detailing decade-long breach where hackers had unimpeded access to Nortel's databases and sensitive information).

[120] *See id.* (discussing hackers breach of Nortel's computer network).

[121] *See id.* (noting hackers had unfettered access to all of Nortel's network).

[122] *Id.* (detailing types of data compromised).

response --they "'did nothing from a security standpoint' to try and keep the hackers out. . . ."[123] Due to Nortel's inaction, the hackers were able to remain in the company's system and continued to monitor its activities.[124]

The breach and Nortel's response likely played a major role in the company's demise.[125] As one expert put it, "[a]s far as I can tell, it's because [Nortel] couldn't win a contract after that because the hackers had their technical knowledge, their financials, their bids before they submitted them. How can you compete in an environment like that?"[126]

V. ISSUES WITH LEGAL REDRESS FOR CUSTOMERS WHOSE DATA IS STOLEN

Theft of sensitive data through sophisticated hacks, rudimentary breaches, and even low-tech means pose a significant threat to private individuals and as shown above, even large corporations and governments.[127] The liability of a corporation both in the courts and the eyes of the public may depend on the sophistication of the attack and the protections in place. A company like RSA that falls prey to a sophisticated attack may be less culpable than a company like Sony,

---

[123] *Id.* (noting Nortel's failure to properly address security breach).

[124] *See id.* (discussing report to then CEO stating that hackers still had access to Nortel's network).

[125] *See* Derek Abma, *Did Hacking Kill Nortel? This Expert Says Yes*, THE VANCOUVER SUN (Feb. 15, 2012), *available at* http://www.vancouversun.com/news/hacking+kill+Nortel+This+expert+says/6157763/story.html (noting data breach as potentially being "the driving force behind the spectacular fall of . . . Nortel. . . .").

[126] *See id.* (discussing Nortel's loss of competiveness due to leaked proprietary and confidential information).

[127] For a discussion regarding the dangers and consequences of data breaches, see *supra* notes 98-126.

which did not implement even the basics of data network security.[128]

Customers seeking legal action against companies that inadequately protected their private data will find that the legal framework leaves little chance for success.[129] This difficulty is the result of procedural hurdles and inability of proving damages caused by the threat of future identity theft.[130] Additionally, current laws only require that companies promptly inform their customers of a data breach but do not create penalties if such a breach occurs, and with the exception of a few states, most laws do not outline any standard for how companies should store private customer data.[131]

---

[128] *See Absolute Sownage*, *supra* note 26 (noting the complete lack of an intelligent security system in place at Sony).

[129] *See* Rancourt, *supra* note 1 at 187-200 (discussing various difficulties faced by plaintiffs in data breach cases and low success rates of such lawsuits). *See also* Hammond v. Bank of N.Y. Mellon Corp., No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *3-*9 (S.D.N.Y. June 25, 2010) (dismissing case because plaintiffs lacked standing due to claimed injuries being "hypothetical and conjectural"); Bell v. Acxiom Corp, No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (noting plaintiff did not sufficiently prove defendant's failure to protect client data caused injuries beyond a speculative nature); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1019-21 (D. Minn. 2006) (dismissing case because plaintiffs were unable to prove damages under theory of increased risk of future harm).

[130] For a discussion regarding the difficulties of litigating customer data breaches, *see infra* notes 132-170 and accompanying text.

[131] *See* Rancourt, *supra* note 1, at 200-05 (discussing inadequacies of current state and federal laws which typically only require notice on part of corporation who inadequately protected customer data). For a discussion regarding federal and state laws *see*, *infra* notes 185-199.

A. COMMON LAW PROBLEMS FOR PLAINTIFFS IN DATA BREACH CLAIMS AGAINST COMPANIES

Customers who wish to pursue legal action against companies that did not properly store and protect their personal data will meet two substantial road blocks significantly reducing their chances at receiving a favorable judgment.[132] The two barriers that have led to almost all related cases being dismissed are standing and proof of damages.[133]

1. STANDING: PLAINTIFFS DO NOT HAVE IT

Standing is a judicially imposed limitation on the legal process.[134] For plaintiffs to have their case heard in court, they must have standing.[135] To have standing, the plaintiffs must establish three elements.[136] First, the plaintiff must have "suffered an 'injury in fact.'"[137] An injury in fact is where a "concrete and

---

[132] *See* Rancourt, *supra* note 1 at 187 (discussing difficulties class action plaintiffs have had in seeking redress for the compromise of their personal data due to failings of defendant companies).

[133] *See id.* at 187, 195 (noting that most plaintiffs' claims fail as a result of lack of standing or inability to prove damages beyond a non-speculative level). *See also* Hammond, 2010 WL 2643307, at *1 (noting that every case court found where plaintiffs sought damages for lost personal data through data breaches have been dismissed).

[134] *See* F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 276-77 (2008) (discussing what standing is and how it functions in the modern American judicial system).

[135] *See id.* at 277 (noting courts have used standing as a means to limit individuals' "ability to invoke the judiciary to vindicate [their] rights.").

[136] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992) (citing Allen v. Wright, 468 U.S. 737, 756 (1984)) (detailing the elements necessary for a plaintiff to establish they have standing in order to seek legal redress).

[137] *See id.* (describing the first element of establishing standing).

particularized" legally protected interest is infringed.[138] Additionally, such injury in fact must be "actual or imminent, not conjectural or hypothetical."[139] Second, there needs to be a "causal connection between the injury [in fact] and the conduct complained of."[140] Lastly, the injury needs to have a likelihood that it will be "redressed by a favorable decision" by the courts.[141]

The norm in most state and federal courts has been to grant motions to dismiss due to lack of standing in cases regarding inadequate security of customer data.[142] The vast majority of cases are dismissed because courts fail to find an injury in fact and thus declare that

---

[138] *See id.* (describing what qualifies as injury in fact). The injury in fact doctrine requires that plaintiffs demonstrate the violation of a legal interest was the cause of a "factual harm." *See* Hessick, *supra* note 134 at 277 (discussing injury in fact rule of standing).

[139] *See Lujan*, 504 U.S. at 560 (noting that such injury must not be conjectural but actual or imminent).

[140] *See id.* (noting that complained injury must be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . the[e] result [of] the independent action of some third party not before the court.") (quoting Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26, 41-42 (1976)).

[141] *See Lujan*, 504 U.S. at 561 (noting that the likelihood of redress needs to be more than speculative).

[142] *See* Rancourt, *supra* note 1 at 187-200 (noting history of courts dismissing such claims). *See also* Madden, *supra* note 12 (noting that courts have frequently held that plaintiffs lack standing because in most cases, plaintiffs can only allege increased risk of future harm).

the plaintiffs lack standing.[143] For example, the Third Circuit in *Reilly v. Ceridian Corp*.[144] dismissed the plaintiffs' claim of increased risk of identity theft due to a security breach based on lack of standing.[145] In *Reilly*, the defendant corporation was responsible for managing payrolls for many clients across the country.[146] Hackers were able to infiltrate the defendant's database system and steal sensitive personal information.[147] The compromised information consisted of social security numbers, birthdates, addresses, and bank account numbers associated with direct deposit.[148] The plaintiffs brought suit alleging that the defendant's inadequate security caused them to suffer an increased risk of future identity theft, emotional distress, as well as the costs of needing to monitor their credit.[149] In affirming the district court's dismissal, the Third Circuit held that

[143] *See e.g.*, Reilly v. Ceridian Corp., 664 F.3d 28, 40 (3d Cir. 2011) (upholding lower court's determination that increased risk of identity theft did not create standing for plaintiffs); Amburgy v. Express Scripts Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009) (holding that risk of future identity theft was not sufficient to establish standing); Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 712-13 (S.D. Ohio 2007) (ruling in favor of defendant's summary judgment motion because plaintiff was not able to establish actual injuries from loss of personal information); Hendricks v. DSW Shoe Warehouse, 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) (dismissing plaintiffs' claim, finding that need for credit monitoring does not constitute actual injury).

[144] 664 F.3d 28 (3d. Cir. 2011).

[145] *See Reilly*, 664 F.3d at 40 (affirming lower court's ruling that plaintiffs lack standing).

[146] *See id.* (discussing defendant's line of work and how it related to plaintiffs).

[147] *See id*. (noting that hackers gained access to sensitive information of approximately "27,000 employees at 1,900 companies").

[148] *See id.* (detailing information potentially accessed by hackers but also noting that it was unclear whether or not "hackers read, copied, or understood the data").

[149] *See id*. (outlining plaintiffs allegations).

there needed to be more than just a speculative or hypothetical possibility of injury, and instead there needs to be a concrete or imminent injury suffered.[150] Furthermore, the court emphasized that because there was no proof that the hackers even stole or understood the data, the imminent nature of the alleged harm was greatly reduced.[151] Accordingly, the Third Circuit affirmed the dismissal, leaving the plaintiffs without a cause of action unless an actual identity theft occurs.[152]

A similar result was reached by the Eastern District of Missouri in *Amburgy v. Express Scripts Inc.*,[153] where the court granted the defendant's motion to dismiss and held that the plaintiffs' risk of future identity theft was not enough to establish standing.[154] There, the plaintiffs alleged that the defendant's inadequate security of its database system allowed "unauthorized persons to

---

[150] *See id.* at 41-43 (discussing holding in *Lujan* and *Whitmore* and reiterating that the mere possibility of future harm is not enough to meet the standing standards).

[151] *See id.* at 43-44 (distinguishing the present case from *Pisciotta v. Old Nat. Bancorp*). In *Pisciotta*, the Seventh Circuit found that standing was established based on the increased risk of future identity theft resulting from a data breach. *See* Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 638-39 (7th Cir. 2007) (holding that standing standard was met by relating data breach related harms to toxic tort where injury has resulted but not yet manifested). For a further discussion of *Pisciotta see infra* notes 164-168 and accompanying text.

[152] *See Reilly*, 617 F.3d at 40 (dismissing plaintiffs' case). It is important to note that the court here distinguished the present case from toxic torts because in toxic torts, the damage had already occurred but manifestation is unexpected, whereas in the present case, no actually damage nor change in status quo occurred. *See id.* at 45.

[153] 671 F. Supp.2d 1046 (E.D. Mo. 2009).

[154] *See Amburgy*, 671 F. Supp. 2d at 1053 (holding that plaintiffs' claim of future threat of identity theft was not enough to establish standing). *See also* Rancourt, *supra* note 71 at 190-91 (discussing court's dismissal of claim for lack of standing even where injuries were "more particularized").

gain access to confidential information."[155] The compromised information included social security numbers, birthdates, and prescription information.[156] As a result of the data breach, the plaintiffs claimed that they suffered an "increased risk of becoming victims of identity theft."[157] Additionally, the plaintiffs claimed that they lost the exclusive use of their prescription information and were forced to continually monitor their accounts in order to prevent potential financial harm.[158] In dismissing the case, the district court stated that an alleged injury must be "actual or imminent, not conjectural or hypothetical."[159] The court importantly noted that there were too many "ifs" that needed to come to pass in order for the plaintiffs to suffer the alleged harm or injury.[160]

Despite the difficulties discussed above, a splintering has begun to occur among the different

---

[155] *See* Amburgy, 671 F. Supp. 2d at 1049 (discussing plaintiff's claims against defendant).

[156] *See id.* (noting type of information which was compromised as a result of the breach of the defendant's network).

[157] *See id.* (detailing plaintiffs' allegations against defendant).

[158] *See id.* (noting plaintiffs' claims of damages and injuries as a result of defendant's inadequate security of its network). *See also* Rancourt, *supra* note 1 at 190-91 (outlining *Amburgy* suit).

[159] *See* Amburgy, 671 F. Supp.2d at 1052 (stating that "[t]he Supreme Court has 'emphasized repeatedly' that the alleged injury 'must be concrete in both a qualitative and temporal sense. The complainant must allege an injury to himself that is distinct and palpable, as opposed to merely abstract, and the alleged harm must be actual or imminent, not conjectural or hypothetical.'") (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)). The court additionally noted that though "imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative. . . ." *See id.* at 1052 (internal quotation omitted).

[160] *See Amburgy*, 671 F. Supp. 2d at 1053 (detailing how plaintiffs' claims were too hypothetical).

district courts regarding standing.[161] While the majority of courts keep true to the injury in fact test of *Lujan*, which requires an actual or imminent harm, some courts have expanded the rule by holding that victims of data breaches can establish standing through potential future harm.[162] For example, the court in *Pisciotta v. Old Nat. Bancorp*[163] found that the risk of future harm did confer standing.[164] In *Pisciotta*, the plaintiffs brought a class action suit against the defendant alleging that because of the defendant's lack of adequate security measures, hackers were able to gain access to the plaintiffs' sensitive personal information.[165] The plaintiffs argued that they were harmed by the increased risk of future identity theft and that they needed to be compensated for credit monitoring services which were needed to protect against potential future identity theft.[166] Breaking from the majority of cases, the Seventh Circuit held that the plaintiffs had standing, stating without much discussion, that the "injury-in-fact requirement can be satisfied by a

[161] *See Hammond*, 2010 WL 2643307, at *1-*2 (noting a split between courts on how to analyze data breach claims against companies).

[162] *See e.g.*, *Pisciotta*, 499 F.3d at 632 (holding plaintiffs have standing because of risk of future harm due to data breach); Krotter v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010) (finding plaintiffs have standing in data breach claim). *But see Reilly*, 664 F.3d at 40 (refusing to follow *Pisciotta* and holding that plaintiffs lacked standing to bring suit); *Amburgy*, 671 F. Supp. 2d at 1053 (holding that risk of future identity theft was not sufficient to establish standing).

[163] 499 F.3d 629 (7th Cir. 2007).

[164] *See id.* at 631 (holding plaintiffs had standing but dismissing case for lack of compensable damages). The court nevertheless dismissed the case because the plaintiffs were unable to prove damages. *See id.*

[165] *See id.* at 631-33 (discussing plaintiffs' allegations against defendant).

[166] *See id.* at 631-32 (discussing plaintiffs' claims and what they sought as damages).

threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[167] Although the court ruled that the plaintiffs had standing, the case was nevertheless dismissed because the court found that the need for credit monitoring did not give rise to compensable damages.[168]

The current state of the law makes it so most cases are unable to make it past the standing barrier.[169] Any cases that overcome the standing hurdle are still likely to be dismissed for failure to prove damages.[170]

2. PROVING DAMAGES FOR POTENTIAL HARM

Some plaintiffs have been able to meet the standing burden if they bring their case in a favorable jurisdiction, but these plaintiffs encounter another roadblock to the successful outcome of their case; proof of damages.[171] Often, the majority of class action plaintiffs will typically not have suffered any actual harm as a result of the data breach but rather a possibility

---

[167] *See id.* at 634 (holding that plaintiffs had standing to bring claim).

[168] *See id.* at 637-40 (dismissing claim for failure to prove compensable damages).

[169] For a discussion regarding standing in data breach claims, see *supra* notes 134-170 and accompanying text.

[170] *See Hammond*, 2010 WL 2643307, at *1 (noting that though some courts will find standing in data breach cases, they are nevertheless dismissed for failure to prove actual damages).

[171] *See* Madden, *supra* note 11 (noting that where cases have been able to make it pass the standing hurdle, claims are typically dismissed for failure to state claim because "potential future harm [is] too speculative to support a claim for damages"). *See also Pisciotta*, 499 F.3d at 632 (dismissing plaintiffs' claims, holding that plaintiffs did have not direct losses or damages as a result of the data breach);

of future identity theft.[172] To survive dismissal, there must be damages that are capable of being redressed.[173] In data breach claims, where plaintiffs are suing the companies for inadequately protecting their personal data, there is usually little proof of exactly what was stolen and in what form.[174] Furthermore, with the exception of those who have actually had their identities stolen, plaintiffs are suing for hypothetical and potential damages.[175]

In *Pisciotta*, the plaintiffs were able to meet the standing burden, but the court still affirmed the dismissal on the grounds that paying for credit monitoring services was not something that could be compensated.[176] In making its determination, the court looked to the law enacted by the Indiana legislature which requires that companies promptly notify their customers if a data breach occurs, but does not create a private right of action or a duty for the company to compensate its

---

[172] *See Hammond*, 2010 WL 2643307, at *1 (discussing typical data breach claims and their lack of actual damages). *See also* Rancourt, *supra* note 1 at 195 (noting that in most cases, data breach victims lack "definitive proof that [the stolen] information has actually been misused").

[173] *See* Shafran v. Harley-Davidson Inc., No. 07 CIV. 01365 (GBD), 2008 WL 763177, at *2 (S.D.N.Y. Mar. 20, 2008) (noting that without more, the "time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy.").

[174] *See* Rancourt, *supra* note 1 at 195 (discussing plaintiffs inability to prove the misuse of stolen data in typical data breach cases).

[175] *See id.* at 195-97 (noting that damages need to be actual rather than speculative for plaintiffs to be able to state a claim which will not be dismissed).

[176] *See Pisciotta*, 499 F.3d at 638 (affirming lower court's dismissal of the case).

customers.[177] Accordingly, the court held that although standing was conferred due to the increased chance of future identity theft, dismissal was still appropriate because of the lack of compensable injuries.[178]

Dismissal due to lack of compensable injuries can be further seen in *McLoughlin v. People's United Bank Inc*.[179] In *McLoughlin*, the plaintiffs brought suit against the defendant for negligence due to lost personal and banking data that arose out of a data breach at The Bank of New York Mellon.[180] The data breach occurred through a low-tech method; the back-up files were stolen off of a truck.[181] The Connecticut District Court was persuaded by the reasoning in *Pisciotta* and found that the plaintiffs had standing.[182] Consistent with the problem in most data breach cases, the plaintiffs had not yet suffered identity theft but were claiming an increased

---

[177] *See id.* at 637-38 (finding that Indiana legislature did not likely intend the costs of credit monitoring to be a form of compensable damages stating "[h]ad the Indiana legislature intended that a cause of action should be available against a database owner for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent.").

[178] *See id.* (affirming dismissal of case because lack of compensable damages).

[179] No. CIV A. 308CV-00944 VLB, 2009 WL 2843269 (D. Conn. Aug. 31, 2009).

[180] *See id.* at *1 (discussing plaintiffs' claim against defendant).

[181] *See id.* (discussing how data breach occurred). It is important to note that though The Bank of New York Mellon encrypted the social security numbers of the defendant's customers on its online database, the backup files were not encrypted. *See id.* Additionally, it can be assumed to be more difficult to orchestra a robbery of physical backups from a company owned truck as opposed to the simple SQL injection hacks that brought down Sony which can be done easily at one's own home. For a discussion of the Sony hacks and methods used, see *supra* notes 25-76 and accompanying text.

[182] *See McLoughlin*, 2009 WL 2843269, at *3-*4 (discussing general move by courts to find standing in data breach cases and accordingly finding that plaintiffs had standing).

risk of potential identity theft.[183] In dismissing the case, the court stated that "the courts of Connecticut, like those of New York, would not recognize a negligence claim founded solely on the fear, unsupported by any allegation of malfeasance, of identity theft. . . ."[184]

B. FEDERAL AND STATE LAW INADEQUACIES

Customers who are unable to bring successful claims under case law will also find the federal and state laws inadequate to address the failure of companies to properly protect their stored private data.[185] The current statutory framework in the United States requires companies to merely inform their customers when their data has been compromised promptly; the majority of laws do not require more of the companies, nor do the

---

[183] *See id.* at *6-*9 (discussing plaintiffs' allegations against defendant and noting pure speculative nature of claims). Additionally, the plaintiffs never alleged what happened to the backup files and it was also unclear whether they were lost or stolen. *See id.* at *1, *7.

[184] *Id.* at *8 (holding that without actual damages, a claim of negligent protection of data could not stand). The court noted that:

> actual damages are a necessary element of any claim sounding in negligence. While no Connecticut Court has ever held that an increased risk of identity theft is insufficient to establish actual damages, the Plaintiffs have pointed to no case decided anywhere in the country where a court allowed a negligence claim to survive absent an allegation of actual identity theft. *See id*.

[185] *See* Rancourt, *supra* note 1 at 200-02 (detailing why individuals bring common law claims against companies for breach of contract and negligence due to the lack of adequate statutory options). *See also* Madden, *supra* note 11 at 27-28 (discussing inability of plaintiffs in data breach cases to successfully bring claims in court).

laws currently address forms of punishment for failure to protect such data.[186]

On the state level, the majority of laws require only that companies promptly notify their customers

[186] *See* Rancourt, *supra* note 1 at 200-202 (noting current federal and state laws focus on hackers not on individuals and also only impose penalties on companies for failure to report, not for inadequate security of their database networks). *See generally* Stored Wire And Electronic Communications and Transaction Records Access 18 U.S.C. §§ 2701-12 (2006) (punishing unauthorized access of stored electronic communications and outlining mandatory and voluntary disclosure of stored communications but silent on storage guidelines or standards); Computer Fraud & Abuse Act, 18 U.S.C. § 1030 (2000 & Supp. 2011) (punishing unauthorized computer access but not defining security guidelines); 15. U.S.C. §§ 6801-09 (requiring financial institutions to disclose when information is compromised). *See also generally* CAL CIV. CODE §§ 1798.80-84 (West 2009) (requiring disclosure for data breach and merely reasonable security measures without defining such measures); DEL. CODE ANN. TIT. 6, §§ 12B-101-04 (2005) (requiring disclosure in case of data breach and giving only Delaware Attorney General authority to enforce); FLA. STAT § 817.5681 (2005) (requiring disclosure when there is a data breach); N.J. STAT. ANN. 56:8-163 (West Supp. 2011) (requiring and defining disclosure and notice procedures if data breach occurs); S.C. CODE ANN. § 39-1-90 (2010) (requiring notice in case of unauthorized access to online databases); VA. CODE ANN. § 18.2-186.6 (West 2008) (requiring notice when data breaches occur). *But see* 201 MASS. CODE REGS. §§ 17.00-17.05 (2008) (requiring "[e]very person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards."); NEV. REV. STAT. § 603A.010 *et seq.* (2010) (requiring encryption of stored data along with disclosure).

when a data breach occurs.[187] Some states have gone further to require that companies encrypt their customer data.[188] The shortcoming of state laws is that the majority do not require any minimum level of security standards, and often do not give customers a private right of action should a company fail to install adequate security measures.[189] Additionally, because most state laws only require prompt notification, once a company notifies its customers of a data breach they no longer are statutorily liable even if they had non-existent security measures.[190] More troubling is that some state laws

---

[187] *See e.g.*, CAL CIV. CODE §§ 1798.80-84 (West 2009) (requiring disclosure for data breach and merely reasonable security measures without defining such measures); DEL. CODE ANN. TIT. 6 §§ 12B-101-04 (2005) (requiring disclosure in case of data breach and giving only Delaware Attorney General authority to enforce); FLA. STAT § 817.5681 (2005) (requiring disclosure when there is a data breach); N.J. Stat. Ann. 56:8-163 (West Supp. 2011) (requiring and defining disclosure and notice procedures if data breach occurs); S.C. CODE ANN. § 39-1-90 (2010) (requiring notice in case of unauthorized access to online databases); VA. CODE ANN. § 18.2-186.6 (West 2008) (requiring notice when data breaches occur).

[188] *See* 201 MASS. CODE REGS. §§ 17.00-17.05 (requiring "[e]very person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards."); NEV. REV. STAT. ANN. § 603A.010 *et seq.* (requiring encryption of stored data along with disclosure).

[189] *See supra* note 186 (noting need to disclose but lack of guidance on security standards).

[190] *See supra* note 186 (creating liability only when companies or entities fail to promptly notify customers of data breach and in some cases only allowing enforcement by Attorney General). *See also* Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467,471-85 (2010) (detailing how many state laws do not allow for private action but rather put enforcement in hands of Attorney Generals as well as exempting companies from notification if information stolen in breach was encrypted).

exempt companies from the need to notify their customers of a data breach if the company used encryption technology to store the data.[191]

Most federal statutes mirror their state counterparts, only requiring that companies disclose to their customers when a data breach occurs.[192] These laws do not detail how companies should store the data nor delineate any minimum standards for companies to follow.[193] The laws create causes of action against the hackers who breached the networks but they remain silent with regard to companies such as Sony who recklessly and negligently store sensitive customer data.[194] Because state laws are nonconforming in their approaches, federal laws may be better suited to address future standards and issues for data security.[195]

---

[191] *See* Joelring, *supra* note 190 (discussing companies exemption from some state disclosure requirements if data stolen was encrypted).

[192] *See supra* note 186 (noting lack of minimal standards for companies in statutes and laws only requiring prompt notice after breach is detected). *See also* Rancourt, *supra* note 1 at 200-204 (discussing inadequacies of federal law).

[193] *See* Rancourt, *supra* note 1 at 200-203 (discussing lack of minimum standards for security in the law but rather focus on punishing those who did hack only).

[194] *See* Rancourt, *supra* note 1 at 201-202 (exemplifying federal law and the creation of criminal liability for hacking databases but lack of standards or guidelines to secure data).

[195] *See* Joelring, *supra* note 190 (advocating for federal statute to control in data breach cases). *See also* Judy Greenwald, *Data Breach Notification Could Benefit From Federal Action*, BUSINESS INSURANCE (Jan. 1, 2012), http://www.businessinsurance.com/article/20120101/NEWS07/301019997 (noting of "growing consensus that federal legislation is needed to address . . . data breach notification. . . ."); Keith Vance, *Keeping Pace with Data Encryption Laws*, eSECURITY PLANET (June 11, 2010), http://www.esecurityplanet.com/trends/article.php/3887111/Keeping-Pace-with-Data-Encryption-Laws.htm (discussing push to enact laws concerning encryption and data protection)

Currently, plaintiffs see little help from state laws in trying to redress their damages as a result of the inadequate security in place by companies, but the tides may be changing.[196] The prevalence of e-commerce, the publicity of high profile data breaches, and privacy concerns has fostered more public awareness as well as legislative acknowledgement of the need for database security.[197] This increase in awareness has led to newer state laws, such as Nevada's, which requires companies that store data encrypt sensitive customer information.[198] Companies should get ahead of this changing legal environment and take the appropriate steps to protect their customer data, not only to prevent future legal liability, but also to maintain customer trust, market share, and profitability.[199]

VI. FUTURE POLICY CONSIDERATIONS FOR COMPANIES

Companies have much to lose if they continue, as Sony did, with minimal or non-existent security measures.[200] Not only do companies face the threat of litigation and the costs that come with a legal defense, they also face loss of market share, customer mistrust, lowered share prices, lost revenue, and even implicit economic costs, such as wasted resources and lost opportunity costs.[201] It is important for companies to

[196] For a discussion regarding statutory inadequacies, see *supra* notes 185-199 and accompanying text.

[197] *See* Greenwald, *supra* note 195 (noting growing interest in need for federal legislation regarding data breaches).

[198] *See* NEV. REV. STAT. ANN. § 603A.010 *et seq.* (requiring encryption of stored data along with disclosure).

[199] For a discussion regarding the benefits of implementing appropriate security measures, see *infra* notes 200-232 and accompanying text.

[200] For a discussion regarding the impacts of data breaches on companies, see *supra* notes 92-126 and accompanying text.

[201] For a discussion regarding the explicit and implicit costs of not implementing adequate security policies and procedures, see *infra* notes 203-217 and accompanying text.

consider these issues before they decide to write off network security as an unimportant expense. The prudent company should instate an effective security policy that will sufficiently protect their customer's data.[202]

A. LEGAL CONSIDERATIONS

Currently, companies creating policies for storing customer data have little to fear by way of litigation for failure to properly protect customer data.[203] As discussed above, plaintiffs bringing claims against companies for security breaches face an uphill battle.[204] Although companies can currently create policies without much fear of legal ramifications, the state of the common law and statutory law are likely to change to reflect the new prevalence of e-commerce and companies should act accordingly.[205] This shift can be seen by the courts that have found standing for potential future identity theft. The changing legal environment is further exemplified by Countrywide's recent settlement for the theft and attempted sale of personal information

---

[202] For a discussion regarding policy and procedure suggestions for database security, see *infra* notes 218-232 and accompanying text.

[203] For a discussion regarding the inability for plaintiffs to successful seek legal redress against companies in data breach cases, see *supra* notes 132-184 and accompanying text.

[204] For a discussion regarding the standing and proof of damages burdens plaintiffs face, see *supra* notes 132-184 and accompanying text.

[205] For a discussion regarding the current common law and statutory environment of data breach claims and the slow move towards new legislation, see *supra* notes 132-199 and accompanying text.

by a senior financial advisor.[206] The Countrywide claim involved an insider at Countrywide who stole millions of customers' information and sold it to third parties.[207] Countrywide agreed to provide two years of free credit monitoring, identity theft insurance, and to pay approximately $3.5 million in attorney's fees.[208] With the potential loss of the legal monopoly companies have on plaintiffs, it would be prudent and cost effective for companies to install more stringent security measures for their stored customer data in order to fend off potential litigation.[209]

B. FINANCIAL AND OTHER COMPANY CONSIDERATIONS

There are financial concerns which should be taken into account when creating security policies which go beyond protecting customer data.[210] As seen in the Nortel case above, companies should have strong incentives to protect the data on their networks.[211] If

---

[206] *See* Matt O'Donnell, *Countrywide Data Theft Class Action Settlement*, TOP CLASS ACTIONS (Jan. 24, 2011), http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/988-countrywide-data-theft-class-action-settlement (discussing recent Countrywide settlement with class action plaintiffs for compromise of sensitive customer data). In the settlement, the attorneys sought approximately 3.5 million dollars in fees alone. *See* In Re Countrywide Financial Corp. Customer Data Sec. Breach Litigation, No. 3:08-MD-01998, 2010 WL 3341200, at *8-*9 (W.D. Ky. Aug. 23, 2010).

[207] *See id.* (discussing claims).

[208] *See Countrywide Data Theft Class Action Settlement Notice*, (Apr. 12, 2010), http://classactionlawsuitsinthenews.com/wp-content/uploads/2010/04/Countrywide-Data-Theft-Class-Action-Settlement-Notice.pdf (outlining terms of settlement).

[209] For a discussion of legal state of data breach claims, see *supra* notes 132-184 and accompanying text.

[210] *See* Rashid, *supra* note 17 (noting that average total cost for company for one data breach is approximately 7.2 million dollars).

[211] For a discussion regarding the Nortel data breach and its financial impacts, see *supra* notes 119-126 and accompanying text.

hackers can gain access to customer data, it is likely that they also have access to sensitive company data.[212] Such a breach can take away a company's competitive advantage, give away proprietary information, give hackers insight into the financial health of the company, as well as drive customers to competitors.[213]

Additionally, data breaches can result in massive losses, as Bank of America saw when the company lost over ten million dollars as a result of a security breach.[214] These losses are particularly disturbing to shareholders because they represent not just lost assets, but also lost opportunities to further shareholder and company interests.[215] Moreover, as Sony exemplifies public exposure of inadequate network security and massive losses of sensitive customer data can result in significant drops in the stock price of publicly traded companies.[216]

---

[212] For a discussion regarding the downfall of Nortel and how the data breach played a major role in the failure of the company, see *supra* 119-126 and accompanying text.

[213] For a discussion regarding data breaches, the types of information that are typically stolen and potential loss of market share, see *supra* notes 92-126 and accompanying text.

[214] For a discussion regarding Nortel's loss of its competitive advantage and eventual bankruptcy, see *supra* notes 119-126 and accompanying text.

[215] For a discussion regarding the financial costs of the data breach of Bank of America as well as the massive financial losses of Sony due to their massive data breach, see *supra* notes 25-91, 113-118 and accompanying text. Additionally, if companies put adequate security measures in place in the first place, they would likely reduce the money spent to remedy such breaches and thus have more money to invest in other areas of the business. It is estimated that approximately forty-one percent of data breaches occur simply due to company negligence. *See* Rashid, *supra* note 17 (noting that negligence is the most common cause of data breaches).

[216] *See Sony Shares Fall Sharply on Data Breach*, CHANNEL NEWS ASIA (May 6, 2011), http://www.channelnewsasia.com/stories/afp_asiapacific_business/view/1127143/1/.html (noting that Sony's shares plummeted in response to the data breaches).

Further, such breaches can endanger the long-term viability of a company by reducing market share, causing a loss of customer trust, and ultimately a loss of a company's customer base.[217]

C. SUGGESTIONS FOR FUTURE POLICIES AND PROCEDURES

Companies should focus on two major areas when creating a security policy to protect stored customer data. First, companies should implement adequate security procedures, such as encryption technologies, to ensure that if a data breach does occur, the data stolen will still be protected.[218] Second, should a data breach occur, companies should immediately notify their customers to allow them the opportunity to protect their identities from possible theft.[219]

1. SECURITY PROCEDURES

Companies' first concern should be to take adequate steps to prevent a data breach from occurring in the first place.[220] Sony had almost no security measures in place to protect their customer data, and their networks were ripped apart in a matter of two months by

---

[217] *See* Rashid, *supra* note 18 (noting customers leaving companies, resulting in a four percent turnover rate, an average 4.5 million dollars loss of business through lost sales and employees being diverted to data breach resolution). For a discussion of the market effects of data breaches, see *supra* notes 200-217 and accompanying text.

[218] For a discussion regarding the need for adequate security procedures, see *supra* 77-91 and accompanying text.

[219] For a discussion of the need to quickly notify customers of a breach, see *supra* notes 77-91 and accompanying text.

[220] *See* Tanya Baccam, *Making Database Security an IT Priority*, SANS ANALYST PROGRAM (Nov. 2009), *available at* http://www.oracle.com/us/products/database/058442.pdf (detailing steps for adequate security of databases).

simple SQL injection attacks.[221] Such an easy breach should not have occurred, especially not against such a wealthy and respected company.[222] Accordingly, companies should take the appropriate steps to prevent unauthorized access.[223] There should be institutional controls designed to prevent unauthorized use of customer files by employees of the company, database security measures in place to prevent known methods of database attacks, and encryption technology should be used on information which is not publicly available.[224] Additionally, companies should have monitoring procedures in place facilitating quick detection of attempted or successful breaches which would allow the company to take the appropriate steps in response to a breach.[225] A company that implements such controls and policies will be better protected from legal liability and will likely not go through the public shaming that Sony experienced if a breach occurs. Indeed, such steps will not only make it more difficult for hackers to access customer data, but they will help reduce potential legal fees, loss of market share, and other financial woes which companies in the past have experienced as a result of negligent database security.[226]

2. AFTER THE BREACH

Not all data breaches are preventable. As was shown in the RSA case, even the most sophisticated

---

[221] For a discussion of the Sony data breaches, see *supra* notes 25-91 and accompanying text.

[222] *See id.*

[223] For a discussion regarding ramifications and examples of such, see *supra* notes 92-126 and accompanying text.

[224] *See* Baccam, *supra* note 220 at 2-13 (discussing methods to effectuate proper security plan).

[225] *See id.* at 10-11 (discussing need and benefits of auditing security systems).

[226] For a discussion of the financial ramifications of data breaches, see *supra* notes 200-217 and accompanying text.

companies can have their databases compromised.[227] Accordingly, companies should have procedures in place to immediately notify customers if a breach does occur.[228] As the Sony case illustrated, notification a week after a breach is unacceptable as a week in the context of data breaches is a life time.[229] Customers need immediate notification so they can quickly take the appropriate measures to protect their identities and financial wellbeing, as well as have a heightened alertness for possible scammers.[230] Such policies will help mitigate the loss of trust which can occur after a customer's data is compromised, and will help to mitigate the outflow of customers to competitor companies.[231] Importantly, failure to quickly notify is currently the one avenue that may expose a company to legal liability, as many state and federal statutes require prompt notification if a breach occurs.[232]

VII. THE TAKEAWAY

When examining the hacker attacks on all aspects of Sony's business, the ramifications for failing to provide sufficient security measures to protect stored

---

[227] For a discussion regarding the highly sophisticated hacker attack on RSA, see *supra* notes 98-106 and accompanying text.

[228] For a discussion regarding the statutory requirements to notify customers of a data breach, see *supra* notes 185-199 and accompanying text.

[229] For a discussion regarding Sony's response to the data breaches and its inadequacies, see *supra* notes 77-91 and accompanying text.

[230] For a discussion regarding the importance of prompt notification after a data breach, see *supra* notes 82-86 and accompanying text.

[231] For a discussion regarding the loss of trust among customers after a data breach, see *supra* notes 200-217 and accompanying text.

[232] For a discussion regarding the statutory need to notify customers if a breach occurs, see *Supra* notes 185-199 and accompanying text.

customer data become clear.[233] It is important to note that although the current legal framework allows companies to be shielded from legal liability for their negligence, they may still incur substantial costs through financial and market share losses.[234] It is also important to note that with the higher prevalence of e-commerce, privacy issues, and the wide publicity of big name company data breaches, the procedural protections companies have may soon be worn away.[235] In the face of the potential consequences when compared to the expenses of implementing appropriate security measures, it becomes clear that companies and customers have a shared interest in the proper protection of sensitive customer data and that companies should take the steps to implement sufficient security measures.

[233] For a discussion regarding the data breaches at Sony and the effects it had on Sony's business, see *supra* notes 25-91 and accompanying text.

[234] For a discussion regarding the legal landscape in data breach claims against companies for negligence and other common law theories, see *supra* notes 132-184 and accompanying text.

[235] For a discussion regarding the changing of state and federal laws, see *supra* notes 185-199 and accompanying text.