Yes, Your Personal Data Is at Risk: Get over It

Marian K. Riedy

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation
Marian K. Riedy, Yes, Your Personal Data Is at Risk: Get over It, 19 SMU Sci. & Tech. L. Rev. 3 (2016)
https://scholar.smu.edu/scitech/vol19/iss1/2

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
Yes, Your Personal Data Is at Risk: Get Over It!

Marian K. Riedy*
Bartlomiej Hanus*

ABSTRACT

Over the past decade, the number of security breaches that have compromised business records containing the personal information of millions of American consumers has soared. The legal world has largely responded in a traditional fashion: by rushing to the courthouse seeking damages for various alleged injuries from the same businesses that had their computers and networks breached by criminal hackers. Corporate misconduct is a classic justification for expending societal resources to hold a company accountable and deter other companies from engaging in similar, harmful conduct. However, company data on consumers and clients may be compromised in situations involving no corporate misconduct. In fact, in many situations the hacker is the primary culprit. The theft of personal information causes minimal harm to consumers, while the business—the putative defendant—suffers far greater costs associated with a breach. Prevention is costly and difficult, and predicting which companies will be hacked, as well as the means by which it will occur, is next to impossible. For these and other reasons, it may be time to consider a data victims’ compensation fund in lieu of private civil litigation. This fund would provide a more efficient and effective mechanism for identifying and exacting financial penalties from only the truly “bad apples”—companies that significantly fail to employ reasonable measures to secure data. Additionally, the fund would provide prompt and fair compensation to individuals harmed by a data breach.

I. INTRODUCTION

In 1984, The Washington Post published a story announcing a data security breach.¹ A few “home computer buffs” stole confidential credit histories from computers belonging to TRW Information Services, a credit bureau; access was obtained through a Sears Roebuck store that used TRW’s

---

* Marian K. Riedy, Esq., is Associate Professor of Business Law in the School of Business at Emporia State University. Before her academic appointment, Dr. Riedy practiced law as a civil litigator in Washington, D.C. She is a graduate of Harvard Law School.

** Bartlomiej Hanus is Assistant Professor of Information Systems in the School of Business at Emporia State University. He received his Ph.D. degree from the University of North Texas. His primary research interests revolve around information security.

services. The thieves gained access to the credit histories of an estimated 90 million Americans, "secured" only by a username and password. The thieves later posted the stolen information on a publicly available Internet board. Although industry analysts surmised that TRW should have readily detected the security breach, company officials were not advised of the breach until a year after its occurrence. The costs incurred by TRW as a result of the breach are unknown. But a search of all reported federal and state cases from the ten-year period following the breach revealed that not even one consumer sued TRW for the unauthorized access of their credit history.

Much has changed since that TRW breach. In today's cyber world, professional hackers, not "home computer buffs," are the principal culprits, and they use sophisticated technology to access data and sell information on the black market. Congress and states have enacted legislation designed to ensure consumer privacy and protect personal information stored in company databases; regulators have adopted relevant rules and standards; companies

2. Id.
3. Id.
4. Id.
5. Id.
6. See id.
7. A search of all reported federal and state cases for the ten-year period following the breach reveals no indication of any filing. As stated elsewhere, in another context, the "first wave" of data security breach lawsuits ensued many years later. See Michael L. Rustad & Thomas H. Koenig, The Tort of Negligent Enablement of Cybercrime, 20 BERKELEY TECH. L.J. 1553, 1556 (2005) (explaining that the "first wave of computer security lawsuits" ensued many years later in another context).
8. See discussion infra Part II.A.
have spent billions of dollars on data security software and systems;¹¹ and a sizeable “cottage industry” selling personal information security services directly to consumers has emerged.¹² All but three states, and the District of Columbia, have enacted statutes requiring companies to notify persons whose confidential personal information has been breached.¹³ Data breaches regularly make headline news stories.¹⁴

The stories of data breaches should come as no surprise. Most consumers frequently swipe their credit and debit cards, and personal information is regularly exchanged on websites like Facebook and eBay.¹⁵ Customers access their retirement accounts and credit reports online and use online bill payment services which house social security numbers, credit card numbers, and account information.¹⁶ We live in the “big data” world of interconnected digital information. While this world is convenient, the numerous threats as-


11. See discussion infra Part II.B.


16. See id.
associated with "big data" should give people pause. It is a fact of life that digitized personal data is continually collected, replicated, transmitted, stored, and used. Any reasonable person should know this information is also subject to misuse.

Of course, knowing does not mean condoning. It is understandable that hacking—an intentional, malicious act—is a crime. Businesses should make reasonable efforts to prevent the theft and misuse of customers' personal information that is collected and exchanged for business purposes. Individuals who suffer actual injuries when their data is stolen and misused should be compensated. However, the dollar value of an injury sustained due to compromised names, addresses, credit and debit card numbers, social security numbers, and other "run-of-the-mill" personal information is usually quite small—less than $99 for most.

Based on the amount of actual injury, then, the usual, large-scale data breach that results in the theft of consumers' personal information from retailers and service providers does not justify a hysterical response. The rush

17. See, e.g., Charles Duhigg, How Companies Learn Your Secrets, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0 (explaining that Target's well-known "pregnancy prediction" data mining, which enabled the company to identify and market specifically to newly-pregnant women, created a stir about the use of very private information for commercial purposes).

18. See id.

19. See Elise Hu, I Feel Nothing: The Home Depot Hack and Data Breach Fatigue, NPR (Sept. 8, 2014, 2:36 PM), http://www.npr.org/sections/alltechconsidered/2014/09/03/345539074/i-feel-nothing-the-home-depot-hack-and-data-breach-fatigue ("You've certainly read the what-to-do-in-the-event-of-a-hack stories here, and elsewhere. How many times have we recommended looking at your credit card bills for any weird purchases, or had security experts remind us to change our passwords, or use two-factor authentication, or not trust the cloud with our most private images?").


22. Id.

23. Of course, not all data breaches are equal. If a foreign government or terrorist group was responsible for or gains access to information from the background checks of millions of U.S. government employees—including contacts with foreign nationals and psychological evaluations, for example—from the breach of the Office of Personnel Management, those employees may be at risk for blackmail, and the foreign nationals for persecution in their home country. See, e.g., Kim Zetter & Andy Greenberg, Why the OPM Breach Is Such a Privacy and Security Nightmare, WIRED (Jun. 11, 2015, 10:40 PM), http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/ (discussing the signifi-
to the courthouse is on, however. Consumers have filed hundreds of data security breach lawsuits that allege dozens of federal and state law claims. Roughly three-quarters of the lawsuits have been class actions.

Consumers whose information has been exposed to security breaches may suffer actual court-redressable injuries.

With the loss of security, consumers may suffer emotional distress worrying about lost privacy and identity risks. They may spend money and time to forestall these dangers by purchasing credit monitoring services, monitoring credit and bank accounts, and seeking to cancel current debit and credit cards. They also may lose opportunities due to unavailable credit or a decline in their credit ratings.

Filing a lawsuit, however, is not always a beneficial remedy. Private civil lawsuits are arguably an inappropriate avenue for those seeking a remedy for data security breaches. The fundamental goal should be preventing data breaches altogether: spending time and resources remediing the theft of less sensitive "commonplace" personal information may do little to advance this goal and be inefficient and unnecessary.

Of course, not all data is equal. Health information in medical records, for example, is considered particularly sensitive. But unlike the theft of "commonplace" information, such as addresses and social security numbers, the large-scale theft of hacked medical information does not seem to cause widespread damage. Thus, while a thief could selectively hack a public figure's health record for the purpose of blackmail or embarrassment, the reasons behind a wholesale hack of medical records—a seemingly remote

cance of an instance where hackers in China gained access to information about U.S. workers with government security clearances).

25. Id. at 100 (identifying 86 unique causes of action from the reported cases, the authors identified 86 unique causes of action).
26. Id. at 83 (reporting that, since 2005, 76% of reported lawsuits for federal data breach were filed as class actions).
27. Carolyn A. Deverich et al., Into the Breach: Plaintiffs Have Been Increasingly Successful in Gaining Injunctive Relief for Online Security Breaches, 34 L.A. LAW. 27, 28 (Feb. 2012) (noting that data breach plaintiffs may also seek equitable relief, such as requiring the defendant to provide plaintiff with the provision of credit monitoring services by the defendant).
possibility—are only speculative. Class action lawsuits arising from the breach of medical history data are not, therefore, clogging the courthouses.

Nor are the consequences of data breach all relatively minor. Consider the following scenario:

[Imagine you are driving at 70 mph in your car when suddenly the windshield wipers go on, the entertainment system clicks on full blast, the horn is honking and the air conditioner starts blowing arctic cold air. Then suddenly you feel the brakes engage. The vehicle is coming to full stop with a freeway full of cars coming up fast in your rearview mirror.]

As it turns out, the vehicle’s control system was hacked. This may warrant some hysteria.

Still, a theft of any data is still a theft, and without a doubt database hacking should not and cannot just be ignored. And theoretically, the threat of litigation by data breach victims should both deter hackers and incentivize companies to employ appropriate security measures. However, there are many reasons why many businesses with client and consumer databases at risk for hacking do not fit into this paradigm. Accordingly, private litiga-
tion may not help. Instead, litigation may undermine the goal of deterrence, do a poor job identifying "blameworthy" parties, and inadequately compensate victims. Therefore, some commentators argue, state legislatures should restrict an individual's private cause of action in tort, as well as statutory rights providing a cause of action. In some cases, those commentators urge providing liability immunity to some companies. Another alternative to a private lawsuit is to create an administered compensation fund to compensate victims of breaches.

Part II of this article examines the phenomenon of data breach: how a breach can occur, the cost presented by a breach, and the prevention mechanisms used. Part III includes a survey of data breach litigation and explores how large-scale hacking-related data breaches differ from other "wrongful corporate conduct," which is the usual justification for private, civil litigation, and proposes, in broad strokes, how state law might be mod-

36. See, e.g., Janet Cooper Alexander, Procedural Design and Terror Victim Compensation, 53 DePaul L. Rev. 627, 648 (2003) ("[T]ort plaintiffs must prove liability, bear the risk that the jury may find against them in the liability phase, pay attorneys fees from any recovery (unless unusual circumstances permit fee-shifting), and enforce the judgment.").

37. See, e.g., S. Rep. No. 114-32, at 10 (explaining that private entities are encouraged by the unwillingness to permit a "cause of action . . . for the monitoring of information systems").

38. See Alexander, supra note 36, at 670 ("[I]mmunity from judicial or administrative review limits the chance that a quick response will be frustrated by second-guessing or litigation over the determination.").


ified to account for such differences. Part IV proposes a more radical change to the current regime: the abolition or substantial reduction in corporate liability for data breach from hacking, and the creation of an administered compensation fund for consumer victims.44

II. DATA SECURITY AND BREACH

The term “information security” comprises three interrelated components: confidentiality, integrity, and availability of data.45 An “information security breach” primarily involves the first two components and occurs when sensitive personally identifiable information46 is accessed without authorization.47

Over the last ten years, data breaches have been reported more frequently,48 due in part to the proliferation and commercialization of Internet technology.49 Additionally, the reporting increase may result from Information Technology (IT) making the subsequent and enduring transformation to market security measures to protect one’s personal data as a service-like commodity.50 In turn, both the resulting increase in interoperability and the exchange of data across various systems51 lead to more data breaches.52 This article provides insight on how breaches occur53 and explores the consequences of those breaches.54 Additionally, this article details the costs asoci-
Your Personal Data Is at Risk

ated with preventing data breaches\textsuperscript{55} and technical reasons why preventive efforts are sometimes unsuccessful.\textsuperscript{56}

A. Breaches and Causes

The number and magnitude of data breaches have risen sharply over the last decade,\textsuperscript{57} more than doubling between 2006 and 2012\textsuperscript{58} and leveling since.\textsuperscript{59} The Global State of Information Security Survey reports that the compound annual growth rate of detected breaches increased by 66% between 2009 and 2015.\textsuperscript{60} This increase in the occurrence of breaches comes with a higher number of compromised records—almost 900 million breached records have been reported since 2005.\textsuperscript{61} However, these figures are approximations because many data breaches either go undetected\textsuperscript{62} or are intentionally unreported by the compromised entities.\textsuperscript{63}

Although determining the frequency of reporting breaches in relation to the total number of breaches is impossible, entities are likely to report breaches more frequently as the rate of breach occurrence steadily rises, particularly where state law requires reporting.\textsuperscript{64} While the public may expect an

\begin{itemize}
\item \textsuperscript{55} Gilstrap, \textit{supra} note 49, at 1279 (citing Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 Mass. Code Regs. 17.00 (2011)).
\item \textsuperscript{56} Derek E. Bambauer, \textit{Schrödinger’s Cybersecurity}, 48 U.C. \textit{DAVIS L. REV.} 791, 844 (2015) (explaining that using preventative software is difficult because the software is complex and can become vulnerable).
\item \textsuperscript{58} Id.
\item \textsuperscript{59} Id.
\item \textsuperscript{61} See Chronology of Data Breaches: Security Breaches 2005–Present, \textit{supra} note 48 (reflecting the number of compromised records, not the number of individuals potentially affected).
\item \textsuperscript{63} See Kamala D. Harris, Att’y Gen., \textit{Data Breach Report 2012}, CA DEP’T OF JUST. 1 https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf (last visited Jun. 2, 2016) (“The cost of breach notification, in hard dollars and reputation damage, has tended to focus the attention of top management and shareholders on data privacy and security practices.”).
\item \textsuperscript{64} See \textit{id.} at iii (“[The Office of the Attorney General] review[s] the information submitted in order to gain an understanding of the types of breaches that are
occasional breach to occur, the actual prevalence may be shocking. In fact, approximately one in five organizations will likely suffer from a material data breach in the next two years.65

There is no “typical” breach—they vary by factors, including:

- the methods used to compromise the data or reasons for the compromise;67
- the number of records compromised;69
- the type or nature of the data accessed;70 and
- the type of organization housing the data.71

But the following non-exhaustive list contains the most common causes of a breach:

- intentional malicious activity or hacking;72
- accidental publication;73
- insider jobs;74
- lost or stolen computers or media;75 and

occurring, what vulnerabilities they may reveal, and what actions might be taken to prevent or reduce the likelihood of future breaches.”).

65. See Hu, supra note 19.


68. See id. at 298 (“The people behind these attacks can be anonymous criminals, insiders intent on revenge, or amateur hackers using automated malware that they could not create on their own.”).


71. Id.

72. See Hu, supra note 19.


74. See Hahn & Layne-Farrar, supra note 53, at 298 (“In addition to the highly skilled malicious hackers who create malware tools, disgruntled insiders can also pose a serious threat.”).

75. See Harris, supra note 63, at 9 (17% of reported breaches occurred because of lost or stolen hardware, and 6% occurred because of lost or stolen media).
Your Personal Data Is at Risk

• patently malfunctioning security measures.76

Intentional hacking results in more stolen or compromised records than all other categories combined.77 A larger data-theft hack might compromise tens of millions of records.78 For instance, recent hacking incidents compromised the confidential account and financial information of:

• 145 million eBay records;
• 130 million Heartland records;
• 76 million JPMorgan Chase client records;
• 80 million Anthem records;
• 77 million Sony records;
• 70 million Target records; and
• 56 million Home Depot records.79

The underlying cause of these breaches is likely a defect in software security system coding.80 An indirect cause, on the other hand, could be human error (e.g., failing to detect a software defect during a security audit,81 or improperly installing or monitoring a security system).82 Regardless of the cause, a “vulnerability” means that “no one . . . is immune to cyber attacks.”83

76. See Oriola, supra note 34, at 463 (“A faulty code or bug is the Achilles’ heel of computer or network systems security, and one of the weakest links through which networked computers are traditionally breached.”).

77. See Chronology of Data Breaches: Security Breaches 2005–Present, supra note 48 (reflecting that more than 70% of record breaches were due to hacking or “unknown”).

78. See, e.g., McCandless et al., supra note 69.


80. See Oriola, supra note 34, at 463 (“A faulty code or bug is the Achilles’ heel of computer or network systems security, and one of the weakest links through which networked computers are traditionally breached.”).


83. See Oriola, supra note 34, at 458, 460 (presenting a discussion of “recent high profile vulnerabilities exploits by malicious hackers within the context of recurring software vulnerabilities imbroglio dictated by the inherent and underlying flaws in software codes”).
Securing against accidental publications (those caused by human error) may be even more difficult than preventing attacking due to software vulnerabilities, due to the fact-specific situations surrounding such breaches. For example, the Australian Immigration Department accidentally disclosed personal details of the world leaders attending the G20 summit in 2015, including passport numbers, visa numbers, etc. The Australian Privacy Commissioner’s Office explained that an employee most likely caused the breach when he mistakenly sent an email containing the sensitive information to the local organizing committee of the Asian Cup.

Similar to an accidental publication, reasons vary widely for a hacking occurrence called an “inside attack.” An inside attack occurred in 2014 when a company consultant for the Korea Credit Bureau stole and leaked personal credit ratings of at least 20 million of the Bureau’s customers, for example. A German Vodafone employee stole approximately two million customer records in 2013. German law enforcement agencies identified and seized the assets from the attacker soon after. Vodafone immediately notified its customers about the breach and cautioned against responding to requests for personal information.

The frequency of incidents related to stolen computers or media (tablets and smartphones, for example) has decreased in recent years, perhaps due to the increased effectiveness of security training efforts. These devices may also be lower-valued targets for theft because of recent advancements in cloud computing and virtualization that allow for the mobility of large amounts of corporate data from employees’ devices to a centrally managed


85. Id.


88. Id.

89. Id.

Breachs related to stolen media or devices are insignificant in terms of volume of data, rarely exceeding a million records, with the majority of reported breaches in the past five years arising from healthcare entities, such as Walgreens, Advanced Medical Group, Sutter Medical Foundations, and Tricare. Some breaches are caused simply by an obvious mistake. For example, a plain error led to the exposure of personal information of 150,000 Citi customers when Citi failed to remove this information, collected between 2007 and 2011, from legal documents before filing those documents electronically on the PACER system. Similarly, in 2014, the Mozilla Foundation exposed about 76,000 Mozilla Developer Network users’ email addresses by running a failing data sanitization process for over thirty days. Even when a specific failure in security measures is not identified as the cause of the breach, under certain circumstances it can reasonably be assumed as the cause. In May of 2015, for example, unidentified criminals downloaded the tax forms of 104,000 taxpayers from the website of the Internal Revenue Service (IRS), using the “Get Transcript” service offered by the IRS on its website.

As noted above, hacking accounts for the compromise of the most records and an estimated 70% of all breaches. Hacking is no longer a leisure activity undertaken by a small group of computer hobbyists; it has become a lucrative business carried out by advanced, well-trained cybercriminals with malicious intent to exploit data for potentially enormous financial gain. For example, the three hackers charged with, inter alia, committing securities fraud on individuals whose identities were stolen from JPMorgan allegedly made hundreds of millions of dollars. Personal information about individuals, such as names, addresses, and social security num-

92. See McCandless et al., supra note 69.
94. See Hem, supra note 73.
95. Jose Pagliery, Criminals use IRS website to steal data on 104,000 people, CNN Money (May 26, 2015, 6:05 PM), http://money.cnn.com/2015/05/26/pf/taxes/irs-website-data-hack/.
96. See Chronology of Data Breaches: Security Breaches 2005–Present, supra note 48 (reporting that over 70% of record breaches were due to hacking or “unknown”).
97. Shahani, supra note 79.
bers, sells for $3 on the black market. The price of financial information, like credit card numbers, as well as PayPal or eBay account credentials, ranges from $10 to $300 per record.

Why any particular company, among the millions of candidates, is selected for hacking is largely unknown. It could well be because that company has porous security measures. In the security industry, it is commonly presumed that hackers engage in “persistent advanced surveillance”: sophisticated hackers roam the networks searching for vulnerabilities and attack when one is encountered. It is also possible that hackers simply target a particular business because someone is paying for the service—possibly a competitor—or for political purposes: the 2010 Symantec Corporation’s global survey showed that half of critical information infrastructure providers experienced politically motivated cyber attacks in 2010. North Korean hackers intentionally hacked Sony, it was widely-rumored, if not proven, because of the pending release by Sony of a comedy show about the assassination of the North Korean leader, Kim Jong-Un.

B. Consequences of Breach

i. Cost to consumers

While a business can estimate and report the overall number of records breached, hackers do not report the percentage of those records they actually misused; available data is scanty. A national survey on identity theft con-


99. Id.

100. Shahani, supra note 79 (suggesting the hackers sought out records of persons who were likely to buy and sell stock).

101. Oriola, supra note 34, at 455 (noting that “software vulnerabilities reputedly account for most of the reported computer or network security problems”).

102. Id. at 478 (“[D]etection research is technically known as software penetration testing, a security and quality assurance testing designed to break into a network to demonstrate that it could be done.”).

103. See Symantec 2010 Critical Infrastructure Protection Study: Global Results, SYMANTEC 5 (Oct. 2010), http://www.symantec.com/content/en/us/about/press-kits/Symantec_2010_CIP_Study_Global_Data.pdf (reporting that “half (53 percent) of all firms said they suspected or were pretty sure they had experienced an attack waged with a specific political goal in mind”).

ducted annually by Javelin Strategy & Research indicates that, in 2012, 22.5% of data breach victims also became a victim of identity theft.\textsuperscript{105} Other research concludes that only a few compromised persons actually suffer any adverse consequence.\textsuperscript{106}

A “back of the envelope” calculation supports the latter proposition. In 2014, a combined 357 million records were compromised due to reported breaches of eBay (145 million), Anthem (80 million), Home Depot (56 million) and JP Morgan (76 million).\textsuperscript{107} Harm from these breaches could, of course, result in a later year. But on the assumption that the thief will work sooner rather than later—before the breach is discovered, before customers are notified of the breach, before credit cards are cancelled—it seems reasonable to assume that more actual harm would be caused at or around the time of the breach.\textsuperscript{108} In 2014, according to the Bureau of Justice Statistics, 17.6 million people experienced an actual financial loss due to a data breach.\textsuperscript{109} Given these figures and these assumptions—admittedly rough—less than 5% of the records hacked were used for any nefarious purpose or at least none that was detected within a reasonable period of time after the breach. In other words, the hackers steal much more data than they use.\textsuperscript{110}

Direct financial loss from the theft can be defined as the “amount the offender obtained from misusing the victim’s account or personal information, including the estimated amount of goods, services, or cash obtained.”\textsuperscript{111} Indirect financial loss includes lost time and money, correcting account information, and all additional costs necessary to remediate the misuse of personal information.\textsuperscript{112} The other major category of damage claimed by victims is


\textsuperscript{107} See McCandless et al., supra note 69.


\textsuperscript{110} See Hu, supra note 19.

\textsuperscript{111} Harrell, supra note 32, at 6.

\textsuperscript{112} Id.
future loss: various costs allegedly arising from an increased risk of, or susceptibility to, data compromise, future data compromise, or identity theft, including the cost of subscribing to credit monitoring services. Victoms also claim damages resulting from the alleged loss of value associated with a wide array of goods and services purchased by the victim from the breached entity. For example, the victim may recover the value of goods bought from Neiman Marcus or the cost of an insurance premium.

For those consumers adversely affected by a breach, the out-of-pocket expense is ordinarily quite small. Given the millions of victims of identity fraud, the overall figures are rather startling: one report found $13.3 billion in losses to consumers between 2005 and 2011, and another report recorded $13.1 billion in 2013 alone. For any one individual, however, the loss is, on average, modest. According to the 2006 Federal Trade Commission Identity Theft Survey Report, the median out-of-pocket consumer expense arising from all identity theft was $0. The median number of hours spent resolving the problem was four. In 2014, according to the United States Bureau of Justice Statistics, one-third of those who had experienced identity theft in that year incurred no identifiable loss, and of the two-thirds who did, one-half incurred an out-of-pocket loss of less than $99. The

113. E.g., the courts’ discussions regarding the allegations of future harm have primarily been centered on whether those allegations give rise to standing. Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015); see also Green v. EBay, Inc., No. 14-1688, 2015 U.S. Dist. LEXIS 58047 (E.D. La. May 4, 2015); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014). Whether and to what extent future harm is a compensable element of damage for any particular cause of action asserted in a lawsuit arising from data breach is a topic beyond the scope of this article. For a discussion regarding the validity of such harm, see generally Rachel Yoo, An Expected Harm Approach to Compensating Consumers for Unauthorized Information Disclosures, 19 RICH. J. L. & TECH. 4 (2012).

114. The plaintiffs claimed they would not have purchased the goods had they known their data was at risk. See Remijas, 794 F.3d at 692.


119. Id.

120. Harrell, supra note 32.
California Data Breach Report of 2014 reports somewhat higher numbers: the average cost to a consumer who fell victim to the fraudulent use of a credit card was $63, debit card $170, checking account $222, and Social Security number $289.121

This minimal economic loss may be explained, in part, by the existence of numerous laws that limit a consumer's liability for certain fraud-related losses122 and those laws that require prompt reporting of data breaches.123 Credit card companies pay for the cost of replacing cards,124 and companies undertake other voluntary efforts to reduce customer loss, such as providing credit monitoring services.125 Not all consumers escape so lightly, however. According to the 2006 Federal Trade Commission Survey, for example, 5% of consumers incur up to $5,000 in out-of-pocket expenses and may spend 1200 hours resolving the problem.126 The 2014 Bureau of Justice Statistics report concluded that 14% of those victims who sustained a financial loss incurred out-of-pocket expenses of $1,000 or more. And while the total loss to any one individual is insignificant relative to the scale of the fraud in its entirety, it is important to note that these losses can be devastating on an individual level; a $500 unreimbursed credit card charge can be catastrophic to a single mother working a minimum-wage job to support three children.127

ii. Cost to the breached entity

On the other side of the equation is the cost to the breached entity. The costs incurred by breached entities generally fall into two categories. The first category of cost is "remediation" of the breach. The company's databases, network, and equipment may have been damaged in the breach and require repair, leading to a temporary disruption of basic business func-

121. Kamala D. Harris, CAL. DEP'T OF JUST., CALIFORNIA DATA BREACH REPORT OCT. 2014, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf. Earlier reports pegged the numbers higher. For example: a Javelin survey from 2004 reported a mean cost per victim ranging from $5,686 to $12,646. Whether the actual loss is diminishing, due to the increased effectiveness of, inter alia, post-breach remedial measures or the differences lie in the techniques of the studies themselves is unknown.


124. E.g., Anderson v. Hannaford Bros. Co., 659 F.3d 151, 164 (1st Cir. 2011) (discussing validity of mitigation costs and noting that many customers had had their credit cards replaced by the issuing bank).

125. E.g., Remijas v. Neiman Marcus Grp., 794 F.3d 688, 690 (7th Cir. 2015).


127. See generally BARBARA EHRENREICH, NICKEL AND DIMED: ON (NOT) GETTING BY IN AMERICA (2010).
tions. The Sony hackers “burned down the house,” according to the company’s CEO: after stealing the data, they wiped the databases and destroyed most of the company’s servers and PCs. In addition to internal “clean-up” and repair expenses, these remediation costs include expenses incurred notifying victims of the breach and replacing their cards. In addition to these direct costs, the entity also typically incurs indirect costs: counter-party and customer business relation expenses, customer churn, and customer loss. Estimates of the overall cost to the breached company vary widely. One widely-cited report shows that the average cost to the company for each stolen record containing sensitive and confidential information is $217 (154 globally), and the average cost per breach is $6.5 million. Another study, based on insurance claims data, reports an “average” of 58 cents per record lost, noting that the cost per record declines as the number of records breached increases.

The second major category of post-breach costs includes fines, penalties, compensatory awards, and attorneys’ fees arising from enforcement action and other litigation. The Federal Trade Commission, for example, may exact civil penalties and consumer redress payments and also may require the implementation of security programs and audits in a successful enforcement action. For example, ChoicePoint, Inc. paid $10 million in civil penalties and $5 million in consumer redress to settle the FTC’s charges in 2006. In 2015, the FTC announced that AT&T had agreed to pay $25 million in connection with an investigation of breaches of several call centers housing the personal data of U.S. consumers. Litigation expenses—excluding reported settlement figures—are almost impossible to quantify because companies do not typically report these numbers separately from other costs. By way of example, Target reported $252 in cumulative expenses post-breach, including litigation and expected liability costs. In any event, although cost esti-

128. Shapiro, supra note 104.
131. FTC enforcement actions involve alleged violations of the agency’s financial privacy and safeguards rules, or unfair or deceptive practices. See generally F.T.C. v. Wyndham, 799 F.3d 236 (3d Cir. 2015).
132. Hughes, supra note 9, at 124.
mates vary, it is universally agreed that the affected businesses suffer—by far—the larger share of the cost of breach, compared to affected consumers, and perhaps as much as 90% of the total loss.135

C. Preventing Breach

Many critics believe companies are simply not doing enough to prevent data breaches. By one estimate, 90% of the data breaches that occurred in 2014 could have been avoided had the compromised organizations simply followed the “best security practices” in the industry.136 But the complete picture is perhaps more nuanced.

The dramatic increase in data breach is occurring despite the fact that the amount spent protecting and securing this data has increased consistently over the years. Continuing the trend, over the next five years, such spending is expected to grow at approximately 2.5% annually,137 and spending on IT security alone is expected to grow by 8.2%.138 Worldwide spending on information security is expected to be near $75 billion in 2015139 and is projected to grow to $101 billion by 2018.140

Perhaps companies should just be spending more to protect consumer data. But money alone will not fix the problem. Data security systems are complex beasts, with multiple vulnerabilities and points of attack.141 And the hackers are only getting better: the complexity and effectiveness of security attacks has been increasing over the years.142 Despite significant advances,

136. 2014 Data Protection & Breach Readiness Guide, ONLINE TRUST ALLIANCE, https://otalliance.org/resources/2014-data-protection-breach-readiness-guide-overview (last updated Apr. 7, 2014) (these practices, for example, would include effective password management, least privilege user access, hardening client devices, regular penetration tests and vulnerability scans, continuous infrastructure monitoring, mobile device management, etc.).
142. Id. at 296.
information security solutions are still primarily reactive rather than proactive in nature. The inevitable consequence of this fact is that a number of data breaches will continue to occur regardless of the amount spent on security.\textsuperscript{143}

Moreover, a business can make substantial investments in security technologies without a significant return because the effective implementation of those technologies is heavily dependent on the availability of specialists in the workforce. As the number and types of security threats grow at a close to exponential rate, it should come as no surprise that there is currently a shortage of qualified cybersecurity professionals on the job market.\textsuperscript{144} Industry experts estimate that the demand for information specialists will soon reach 6 million globally, with an expected shortfall of 1.5 million persons.\textsuperscript{145} This gap is even larger for top-level cybersecurity experts, or those who design and manage the deployment of information security initiatives in large organizations.\textsuperscript{146} If the supply-demand gap were closed, however, the industry would still suffer from the lack of clarity and standardization in data security standards.\textsuperscript{147} Colleges and universities struggle to create cyber security programs that meet industry needs without a clear and consistent definition of what those needs are.\textsuperscript{148}

Given the constraints and the unknowns, it could perhaps be concluded that in regards to preventing data breaches from hacking—as opposed to obvious mistakes and internal errors—a company should be expected to meet any specific standards set forth by its industry,\textsuperscript{149} remain abreast of developments in technology and knowledgeable about the latest in hacking techniques, and strive for continuous improvement. That a company should have met any one security expert’s opinion as to what security measures are “rea-

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{143} Bambauer, \textit{supra} note 56, at 844 (“Complete prevention of inaccuracy is impossible . . . [s]oftware code displays extraordinary complexity, leading invariably to bugs. Hackers are adept at finding and exploiting vulnerabilities.”).
\item \textsuperscript{145} See id.
\item \textsuperscript{147} See id.
\item \textsuperscript{148} \textit{Closing the Cybersecurity Workforce Gap}, \textit{SYMANTEC OFFICIAL BLOG} (July 7, 2014), http://www.symantec.com/connect/blogs/closing-cybersecurity-workforce-gap-0.
\item \textsuperscript{149} See \textit{id}.\textsuperscript{e.g., Framework for Improving Critical Infrastructure Cybersecurity}, \textit{NAT’L INST. OF SCI. AND TECH.} (Feb. 12, 2014), http://www.nist.gov/cyber framework/upload/cybersecurity-framework-021214-final.pdf (noting this would be a general example of an appropriate security standard).
\end{enumerate}
\end{footnotesize}
sonable," expressed in the context of a negligence lawsuit or otherwise, may just not be a reasonable or feasible expectation. And whether it is 10% or a significantly higher figure, a number of data breaches simply could not have been avoided even by employing the "best practices" of information security.

A final point on spending for security measures should be noted. The increased spending on security measures may not yet be stemming the tide of breaches, but it does decrease the costs to companies once a breach occurs. In addition to employing technical countermeasures like encryption, post-breach costs can be minimized by having IT security functions strongly aligned with business operations (top management involvement, well-defined business continuity, disaster recovery procedures, employee awareness and training, etc.). For example, a well-trained incident response team may on average reduce the cost of responding to a data breach by almost $24 per record. Proper technology countermeasures and business continuity planning demonstrably reduce the cost of responding to a breach.

D. In Sum

For the most part, data security breaches are caused by criminal activity over which the breached entity has absolutely no control. A company may become the target of an attempted breach because it has failed to employ reasonably acceptable security measures, has done or said something "unpopular," or simply by random chance. Protecting confidential consumer data against breach is a steep and growing cost to businesses, and it is difficult, if not impossible, to determine how much is enough. The breached entity bears far the lion’s share of the cost of a successful breach: the consumer, not so much.

III. THE LITIGATION LANDSCAPE

This section, in broad strokes, describes the world of private litigation on behalf of consumers affected by a data breach. It then discusses why private litigation is an inapposite solution given the "how and why" of data security breaches.

150. Proving whether or not the breached company had met some ill-defined "industry standard" would be just a "battle of the experts," the outcome of which would be uncertain. In re LinkedIn User Privacy Litigation, Case No. 5:12-cv-03088-EJD, 309 F.R.D. 573, 587 (N.D. Cal. 2015) (discussing the strengths and weakness of the plaintiffs' case in evaluating proposed settlement agreement).


breaches and proposes minor, but possibly significant changes to common law remedies for data breach.

A. The Data Breach Lawsuit

According to one study, between 2005 and 2010, there were sixty-five data breach lawsuits in U.S. federal courts where plaintiffs alleged a compromise of their personal information. 153 76% of these lawsuits were class actions.154 A search of reported decisions from 2011 through 2015, using the same search terms as used in that study, returns at least sixteen such cases in federal courts.155 It seems fair to assume, particularly during the initial stages of a lawsuit, that the number of reported decisions would be a small subset of the number of cases in suit. Given the increases in the number of reported breaches over the last few years, and keeping in mind that not all data breaches can be prevented, regardless of the security measures enacted,156 it can safely be concluded that these cases will continue to plague the judicial system. “Plague” seems a fair word to use, since these cases are typically mammoth undertakings involving complex legal and factual issues. As one court presiding over a data breach lawsuit stated, “as evident from the instant action, this climate undoubtedly raises a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future.”157

By way of example only, In re Target158 arose from a massive data breach in which computer hackers gained access to credit and debit card information, and other personal information for approximately 110 million customers.159 Lawsuits were filed by the consumers whose data was swiped and by credit and debit card issuing companies, claiming damages for costs

153. Romanosky et al., supra note 24, at 84 (noting that the plaintiffs alleged a breach of “their” personal information, suggesting that most, if not all of these lawsuits were brought by individual consumers, not by competitors alleging theft of trade secrets, insurance companies, or other putative plaintiffs.).

154. Id. at 83.

155. The LEXIS database was used for this search (emphasis added).

156. See discussion infra Part II.D (noting most breaches are out of the control of the company).


159. Id. at 1157.
of replacing cards and reimbursing fraudulent charges. The complaint in the consumer plaintiff class raised claims under the consumer protection laws of forty-nine states and the District of Columbia; these laws differed in terms of, inter alia, whether a private right of action was created, what kind of injury justified redress, and whether the claim could be brought as a class. The complaint contended that Target violated data breach notification statutes in thirty-eight jurisdictions and asserted various other state law claims, the elements of which varied considerably from state to state. The Target case is not unusual in the complexity of the claims. Data breach complaints, in general, "allege a staggering range of both common-law (tort, breach of contract) and statutory causes of action." This reported range includes eighty-six unique causes of action. For example, the consumer plaintiff class in the Sony breach litigation brought fifty-one independent causes of action.

This complexity arises, in part, because the defendant in a federal data breach lawsuit has a national presence and therefore customers or clients in many states. But even "run-of-the-mill" lawsuits filed in state courts involve multiple and overlapping claims. Thus, in Stanturf v. Amerigroup, a plaintiff class composed of an alleged 400,000 Kansas residents sued a group of insurance companies for data breach, raising ten claims based on state law.

160. Id.; see generally In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 484 (D. Minn. 2015).
161. In re Target, 66 F. Supp. 3d at 1161.
162. Id. at 1166.
163. Id. at 1171. The court noted, however, that the elements of the breach of contract and unjust enrichment claims were substantially similar in the various applicable jurisdictions.
165. Romanosky et al., supra note 24, at 76.
167. This phenomenon is not limited to data breach cases, of course. In arguing that state law claims for deceptive advertising should be preempted by federal law, the author noted: "In this day and age, most advertising is nationwide and most harm suffered is thus also nationwide." Stacey M. Lantagne, A Matter of National Importance: The Persistent Inefficiency of Deceptive Advertising Class Actions, 8 J. BUS. & TECH. L.J. 117, 118 (2012).
169. Plaintiffs cobble together various state law claims because there is no federal or state statute specifically creating a claim arising from breach of a consumer's
The composition of the parties is also likely to be complex for several reasons. First, the consumer plaintiff class is likely to be large. Certainly a class of 400,000 putative consumer members is not unmanageable, and the class can of course be much smaller. But the larger the class, the larger the overall award will be in event of settlement or verdict. Empirically, the larger the data breach—and thus the larger the potential class—the greater the probability that the case will be litigated. In other words, it is more likely that the consumer plaintiff class will be large because smaller putative classes will simply not end up in court.

Second, damage caused by a significant data breach can spread beyond the individuals whose personal data has been compromised. A class of credit card issuers sued Target as a consequence of that breach, as did Target shareholders. Liability may extend far beyond the entity suffering the breach, and the number of and relationship among putative defendants may create another complication in the suit. Target’s security software auditor was sued alongside Target following that breach. The breach of an estimated 80 million Anthem health care records could ensnare nearly sixty health insurance plans from all over the United States. These entities have contractual rela-

digitized personal information. As discussed in more detail below, various federal statutes, including HIPAA, impose data security requirements without providing for a private cause of action for damage resulting from a data breach. Similarly, state consumer protection statutes may or may not provide for a private cause of action, and because these statutes were not enacted to address data breach, whether and to what extent these provide consumer redress are ongoing issues of interpretation.


171. Lisa L. Casey, Reforming Securities Class Actions from the Bench: Judging Fiduciaries and Fiduciary Judging, 2003 B.Y.U. L. REV. 1239, 1241 ("As a general matter, the larger the company sued (as measured by market capitalization), the larger the losses suffered by the putative class, and the larger the potential settlement fund.").

172. Romanosky et al., supra note 24, at 83.


174. Pletz, supra note 81.

tionships with Anthem to facilitate a national payment network, and these relationships may result in an extension of liability for the data breach.\textsuperscript{176} Businesses and their data are increasingly interconnected in the global economy, posing the risk that a data breach of one will implicate many.

At the end of the day, the case may well be settled. The settlement rate for federally-litigated lawsuits appears to be about 50\%.\textsuperscript{177} From the handful of publicly available reports on how these settlements are disbursed, claimants receive modest amounts, commensurate with what studies demonstrate would have been their actual losses.\textsuperscript{178} Also, because of the negligible monetary loss, it seems likely that only few within a class actually submit claims. In the \textit{LinkedIn} data breach litigation, the settlement netted $14.81 for each of the roughly 6\% of the class making a claim.\textsuperscript{179} In the \textit{Heartland} case,\textsuperscript{180} 290 claims were submitted from a class of over 100 million and only eleven were deemed valid.\textsuperscript{181} Only $175 was paid per claimant for a total payout to consumers of about $2,000.\textsuperscript{182} According to an empirical study of settlement payouts for data breach cases litigated in federal courts between 2005 and 2011, the mean value of settlements awarded to plaintiffs was about $2,500 per plaintiff, with most awards being a nominal amount of approximately $500 and often awarded to named plaintiffs only.\textsuperscript{183}

\section*{B. A Data Breach Lawsuit?}

The picture painted thus far probably appears little different from the “standard” consumer class action. Class actions are by nature large, expensive, and messy affairs often launched against entire industries.\textsuperscript{184} In so-

\begin{enumerate}
\item \textit{Id.}
\item Romanosky et al., \textit{supra} note 24, at 84.
\item Deverich et al., \textit{supra} note 27, at 5.
\item In \textit{re LinkedIn} User Privacy Litigation, Case No. 5:12-cv-03088-EJD, 309 F.R.D. 573, 581–82 (N.D. Cal. 2015).
\item \textit{Id.} at 1050.
\item Romanosky et al., \textit{supra} note 24, at 100. It should be noted that unclaimed funds would be spent as per the terms of the settlement agreement, on payments to non-profit organizations, for example. \textit{See generally} Christine P. Bartholomew, \textit{Saving Charitable Settlements}, 83 FORDHAM L. REV. 3241 (2015).
\item E.g., Eric A. Poster, \textit{Tobacco Regulation or Litigation?}, 70 CHI. L. REV. 1141 (2003) (reviewing W. Kip Viscusi, \textit{Smoke-Filled Rooms: A Postmortem on the Tobacco Deal} (2002)).
\end{enumerate}
called “small stake claims,” or when individual damages are low, it necessarily follows that each member of the class will receive a modest or token amount for compensation. Generally, after a settlement, the number of actual claims made by the class is small. In fact, “[s]ome class members never learn of the settlement or forego filing claims. Even with directly mailed settlement checks, some are returned or never cashed.”

Despite the large, overall cost and the potentially small payout to individual plaintiffs, the class action theoretically benefits society. Much has been written about those potential benefits, and it would be impossible to address all the arguments made about the positive effects of this procedural vehicle. Aggregating a number of small claims creates a potential pay-off sizeable enough to encourage attorneys to prosecute these cases. Thus, as a class, injured parties can serve as “private attorney generals,” enforcing laws that are otherwise flouted. And in prosecuting the case, plaintiffs’ attorneys may discover corporate wrongdoing that would otherwise go undetected. Regarding small stake claims, class actions are justified because they “level the playing field” and allow individuals “to seek redress for

185. Bartholomew, supra note 183, at 3248.


187. E.g., Kline v. Coldwell, Banker & Co., 506 F.2d 226, 237 (9th Cir. 1974) (of the 400,000 members the plaintiffs claimed to be representing, only one submitted a claim).

188. Bartholomew, supra note 183, at 3248.

189. E.g., Eran B. Taussig, Broadening the Scope of Judicial Gatekeeping: Adopting the Good Faith Doctrine in Class Action Proceedings, 83 ST. JOHN’S L. REV. 1275, 1277 (2009) (“A vast body of literature has been written about the problems and abuses of the class action procedure.”).


191. E.g., Opderbeck, supra note 186, at 1688–89 (“Private attorney generals” is the well-known term used to describe actions brought by private plaintiffs to enforce laws that would, theoretically, go unenforced or at least under-enforced if left to government action.).

192. See Bohn & Choi, supra note 190, at 906–07.
wrongful corporate conduct” by bringing claims that would otherwise be too small to pursue.193

In very broad strokes, the other side of the argument is that class action is “a mechanism for plaintiffs’ attorneys to extract rents from the corporate treasuries of defendant firms and insurance companies.”194 Assume, arguendo, that there is some validity to this position—that small claims class actions are an expensive and clumsy vehicle for redressing widespread but minor economic injuries. Nonetheless, if the benefits of the class action vehicle outweigh the negatives, there would be no justification for curtailing or prohibiting the use of the class action. If the arguments in favor of the class action are particularly weak in regard to certain types of corporate “wrongdoing,” however, the balance would be struck against using the class action for these cases, in particular. What follows, then, is an analysis of the “wrongdoing” that leads to compromises of personal information caused by hacks into the data networks housing that information. An incident in which a company accidently uploads files with personal customer data onto a publicly available website195 is another issue and another discussion, entirely.

i. Are data breach defendants the “wrongdoers”?

In consumer data breach lawsuits arising from hacking, the defendant company is not typically the true “wrongdoer.”196 The cybercriminal who hacks the database and then sells or uses the data is the true culprit. Of course, a defendant can be liable for injury arising from criminal conduct if the defendant’s negligence is the initiating cause and the injury is reasonably foreseeable.197 A landlord can be liable for a theft from a leased apartment of the tenant’s laptop computer if the landlord is negligent in providing security measures for the apartment, and the theft is reasonably foreseeable.198 But in the data breach cases, the thief has broken into the landlord’s house and stolen the landlord’s computer, which contains a tenant’s personal information. It is the company’s property (databases and networks containing customers’ personal information but also potentially company trade secrets and other


194. Bohn & Choi, supra note 190, at 907.

195. See discussion supra Part II.A.

196. One of the named plaintiffs in the Heartland case objected to the settlement on the grounds that, because the consumers had not actually been harmed by the breach, the settlement was unfair to Heartland. In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 851 F. Supp. 2d 1040, 1050 (S.D. Tex. 2012).


198. Id.
confidential and business information) that has been breached. The company is the primary "victim."

The defendant company is also the main "victim" in other ways. It is the company that becomes the target of nasty headlines, an FTC investigation, and shareholder derivative actions. It is the company that pays the costs of responding to the breach, repairing the breach, and notifying affected customers. The company is the victim that incurs third-party costs, such as payments to credit card companies and higher premiums for security breach insurance.

The fact that both the breached company and its customers have been injured does not and should not preclude assigning fault to the company if the company's security measures were faulty. It should be noted, however, that the efficacy of those security measures are, to some extent, a product of external factors beyond a company's control. First, as noted in Part II.B, the security technology specialists who install the data security software and system are in short supply. Second, vulnerabilities in security software are among the most common entry points for hackers. Companies purchasing security software generally rely on the vendor for data protection. If that protection fails, the breached company pays the piper and typically has little or no recourse against the vendors who have contractual protections against such liability. Further, the security software market is a consolidated market, meaning that one vendor will serve a multitude of companies. Most cyber security vendors promote customer success stories indicating that their customers represent a vast array of industries and markets. All of those companies have taken the same precautions against breach. Some of those companies will be targeted, and others will be randomly hacked. The victimized companies will be accused of negligence and other wrongful acts. One might ask why, under these circumstances, only the unlucky few should be called out in class action lawsuits. The responsibility for a breach may alternatively lie with parties other than the software vendor. The fault may, for example, lie with the person who installs the software or links the software to

199. See S. REP. No. 114-32, at 3 ("Moreover, it is these same companies who are the victims of malicious cyber activity, and their appropriate efforts to protect themselves and other future victims from cyber threats should not only be authorized but protected from unnecessary litigation.").

200. See generally supra Part II.C.2.

201. See Oriola, supra note 34, at 455.

202. See id. (discussing how "software vulnerabilities reputedly account for most of the reported computer or network security problems"). But see Olavsrud, supra note 82.

203. See Gilstrap, supra note 49, at 1272–73.

Given this "complex set of interdependencies" comprising a data security network, it is certainly not evident that the breached company should bear the liability. But it is the breached company that becomes the target for consumer lawsuits: Target and Sony are in the headlines and not the external custodians of their security networks.

It is fair to assume that it is a well-known fact that security software can fail. Thus, it might be argued that, in addition to diligently patching systems for known vulnerabilities, all companies should take additional measures to prevent breaches. This cost will presumably be passed to consumers. Whether the additional cost is justifiable is uncertain. In contrast, what security measures a landlord must employ depends largely on whether the leased apartment is in a "high crime area." If the risk is high, the landlord is expected to account for this heightened risk. In the murky world of data breach, attacks can be random and unpredictable. What is a "high crime" area is impossible to determine. Generally, one might reasonably argue that data breaches and subsequent harm to customers are "foreseeable" because of the overall frequency of breach, but in the specific case of any one "landlord," perhaps not.

There is also the issue of causation when some measure of fault is assumed. Regarding cause-in-fact, given that digitized personal information is usually distributed widely (over the course of a year a consumer will swipe her credit or debit card hundreds, if not thousands of times), how likely is it that any one fraudulent transaction can be securely linked to any one particular breach? When a card is swiped, the data could be hacked by the clerk handling the card, if not by a criminal hacker. That breach may never be detected or, if detected, never reported.

Legal criteria could surely be devised to assign liability to one of the entities through whose networks the digital information has passed. For example, the old common law rule, which applies when a plaintiff has clearly

---


206. For example, Target and Sony are in the headlines for bearing liability, but they are not the external custodians of their security networks. Id. at 329.

207. See Bambauer, supra note 56 ("Additionally, information asymmetry means that defenders are always behind.").

208. Panel Round One (NPR radio broadcast Dec. 19, 2015), http://www.npr.org/2015/12/19/460332256/panelroundone (stating that during a heavy shopping season, a card may be swiped dozens of times over a very short period of time, leaving a "trail of personal information" while shopping for the holidays).

209. See Remijas v. Neiman Marcus Grp., 794 F.3d 688, 696 (7th Cir. 2015) (rejecting this argument when raised by the defendant Neiman Marcus, but in a different context and based on a different standard: the issue was whether the injury was "fairly traceable" to the data breach for showing standing to sue).

210. E.g., Resnick v. Avmed, Inc., 693 F.3d 1317, 1327 (11th Cir. 2012) (stating that courts are adopting approximate time limitations between the date of the
been injured but the specific wrongdoer cannot be identified, could govern. 211  
The burden of proof then shifts to the defendant to prove that the information was not stolen from its databases. But in the interconnected data world, one might fairly question whether this is fair and reasonable. On occasion, the answer may be yes, as when a criminal investigation uncovers a massive scheme to hack a specific set of data from a particular company in order to obtain contact information of specific investors. 212 But for the run-of-the-mill data breach from a retail store, it seems mostly a guess as to whether the breach giving rise to a lawsuit caused the subsequent identity thefts, or whether these resulted from some other data transfer.

Proximate cause is also problematic. As noted above, very little is actually known about what cybercriminals do with all the purloined data unless a criminal investigation brings it to light for a particular case. 213 Arguably, the “standard” injuries—credit and debit card fraud, opening of fraudulent accounts, and damaged credit ratings—are reasonably foreseeable. But when other, more “exotic” damage occurs, such as the “pump and dump” security fraud devised by the hackers of JPMorgan Chase’s data, 214 the breached company might legitimately be as surprised as the injured customer.

And finally, what responsibility should the customer bear? Today, it would be the unusual customer who is unaware that digitized personal information is readily transferrable and replicable, persists forever, and can easily be accessed. 215 This is not to say that consumers voluntarily assume the entire risk of data compromise when they exchange their personal data for goods and services, but it is at least a known risk. It could therefore be argued that customers voluntarily surrender at least some fraction of their security and privacy for convenience by storing their credit card number with the vendor instead of using alternative, “safer” (but often significantly less convenient) payment methods. Further, given the number of publicized data breaches, a rational person should at least entertain the possibility that he or she might become a victim of a data breach. Perhaps it is not unfair to expect customers to accept some rather minor, unpleasant consequences as a necessary cost of convenience. After all, the faint of heart could purchase individual identity theft insurance, and any customer notified of a data breach should be expected to take appropriate steps to mitigate harm. According to the 2015 Identity Fraud Report issued by Javelin Research & Consulting, two-thirds of

breach and the date of the unlawful use of the data, beyond which causation is too speculative).

211. *E.g.*, Summers v. Tice, 199 P.2d 1, 5 (Cal. 1948).

212. Shahani, *supra* note 79.

213. *See id.*

214. *Id.*

identity fraud victims had received notification of a data breach.216 Perhaps nothing could have been done to prevent the initial data compromise from becoming data misuse. But perhaps too many just did not take the time to do anything to protect themselves from harm.

ii. Are these lawsuits necessary?

It is with some hesitancy that one leaps into the discussion of whether data breach lawsuits are an appropriate means of encouraging companies to employ better data security systems. The answer depends, fundamentally, on one great unknown: whether the threat of a lawsuit, and its attendant publicity and costs, are significant factors for corporate decision makers in choosing security products.217 But a few other considerations suggest that private lawsuits may be an impediment to improving data security, at worse, and in any event largely unnecessary, at least in light of the associated costs.

First, effective data security requires continual innovation. Measures that encourage companies to share information about perceived and actual security threats, and to cooperate in developing new technologies, are likely to improve data security for all.218 For example, Google in July 2014 introduced Project Zero, a program that uncovers, reports, and fixes previously undisclosed computer software vulnerabilities.219 But the threat of litigation may weaken overall data security by discouraging companies from sharing security vulnerabilities.220 A company is not likely to disclose information on a security “failure” when that information could be used as evidence of negligence.221 Thus, “the specter of litigation for monitoring a company’s own...
networks or sharing cyber threat indicators or defensive measures for cyber-
security purposes has disincentivized private sector cybersecurity efforts."222
Also, a data security system comprises many distinct entities: security
software programmers and vendors, system auditors, and ISPs, in addition to
the company in the business of collecting and using consumer data. Imposing
liability on the wrong party, or only on the business, "could result in weaker
overall security by undermining incentives to take precautions."223

Second, companies have strong incentives, unrelated to litigation, to
devote money and resources to employing effective security measures. One
incentive is that businesses must invest in data security measures to protect
their own data, including trade secrets and other proprietary information.224
Another incentive is the cost incurred by a breached entity when responding
to a breach.225 As discussed in Part II.C, this cost is substantial.226 The cost of
notification alone is an incentive for preventing breach. Thus, "the cost of
breach notification, in hard dollars and reputation damage, has tended to fo-
cus the attention of top management and shareholders on data privacy and
security practices."227 Avoiding a breach is in a company's financial best
interest, regardless of the threat posed to companies from consumer class
actions. There are, no doubt, financial and other reasons for companies to
"cut corners," or even consciously refrain from employing certain security
measures because too much security can harm the business.228 But a com-

224. Id. at 323–24 ("Many firms, however, do appear to have significant incentives
to protect their systems. Companies with truly vital systems generally ‘air gap’
them—meaning that those systems are not linked directly to public networks
and are therefore not exposed to externalities in security. Others with valuable
databases and sensitive files have strong incentives to protect their networks
from attack in order to guard their investments and their reputations.").
225. This fact seems overlooked when it is claimed that only the individuals whose
personal information has been compromised directly incur harm, and when it is
argued that companies are therefore dis-incentivized to spend appropriate
amounts on data security. E.g., Danielle Keats Citron, Reservoirs of Danger:
The Evolution of Public and Private Law at the Dawn of the Information Age,
226. A portion of these costs arises directly from legal obligations imposed on the
company: notifying customers of the breach, reimbursing for fraudulent credit
card charges, replacing credit and debit cards, and etc. A failure to comply with
these obligations could also result in a lawsuit or regulatory enforcement ac-
tion. So the threat of litigation is certainly not irrelevant. What is discussed in
text is the separate deterrent effect of a private consumer lawsuit arising from
the breach itself.
227. Harris, supra note 63, at 1.
228. E.g., Jose Pagliery, Why Retailers Aren't Protecting You From Hackers, CNN
MONEY (Feb. 18, 2014, 6:56 AM), http://money.cnn.com/2014/02/18/technol
pany’s failure to prevent a breach does not closely fit the classic paradigm of “corporate misconduct” that class actions are intended to deter: cutting safety features on a design of a car to manufacture and sell it more cheaply, for example.\textsuperscript{229} In data breach situations, the corporate executives are passengers in the car.\textsuperscript{230}

But what of those companies that do cut corners, or simply cannot afford the costs of an adequate data security system? Are class actions still needed because of their role in “uncovering” specific instances of corporate misconduct?\textsuperscript{231} To some extent, the data breach notification statutes accomplish this objective. These statutes have “opened a window on privacy and security practices.”\textsuperscript{232} Certain types of breaches must be reported. When and how a breach must be reported varies by jurisdiction. Thus, full disclosure of breaches can never be assumed. Whether a company has fully and fairly disclosed such breaches should be monitored. But strengthening these statutes and having regulatory oversight of compliance could, perhaps, well serve the goal of deterring breaches. Ensuring that consumers are notified of a breach would also further enable consumers to take “self-help” measures to prevent or mitigate damage, which in turn would reduce the need to race to the courthouse.

Another consideration, in assessing whether class actions are a needed inducement to protect customer data, is that many companies are subject to specific regulatory requirements. For certain industries, the requirements are fairly specific. For example, the Gramm-Leach-Bliley Act requires financial institutions to develop a written information security plan describing how their program protects consumer information.\textsuperscript{233} Similarly, entities covered by the Fair Credit Reporting Act are required to safely dispose of consumer reports.\textsuperscript{234} Even general retailers are subject to Federal Trade Commission

\textsuperscript{229}. This is a reference to the infamous Ford Pinto case.

\textsuperscript{230}. In fact, it is generally assumed in the industry that companies employ stricter security measures on customer and client data than on corporate data: the customers are in the safest seat in the car.

\textsuperscript{231}. Bohn & Choi, \textit{supra} note 190, at 948 n.153.

\textsuperscript{232}. Harris, \textit{supra} note 63, at iii (under Cal. Civ. Code § 1798.82, for example, the state obtains information on the types of breach, what “vulnerabilities” the breaches reveal, and what action might be taken to protect against future breaches).

\textsuperscript{233}. See Rosenfeld & McDowell, \textit{supra} note 9, at 90.

\textsuperscript{234}. \textit{Id}.
enforcement actions if the company has "engaged in unfair or deceptive trade practices that put consumers' privacy at unreasonable risk." Between 2002 and 2014, FTC brought fifty such actions.236

Lastly, one might question how, exactly, does the threat of a private lawsuit motivate companies (those that are not obviously "bad apples") to do more than they are already doing? Just how much more is society willing to pay in an effort to prevent fraudulent credit and debit card charges? That is, fundamentally, what the Target, Anthem, and the Home Depot lawsuits are all about: those companies didn't do enough to prevent a few dollars in individual harm. Litigation costs time and money.237 If the parties settle, the cost of attorneys' fees; the cost of employee time spent on investigating, responding to allegations in the complaint, and responding to discovery requests; the cost of expert witness fees; and other pre-settlement costs must be added to the cost of administering the proceeds. For example, Heartland probably spent $160,000 per valid claim made while administering that settlement fund, including the cost of notifying claimants of the settlement, for a mere $175 payout to each victim.238 Such a process expends judicial resources. Some portion of costs to the company defendant will be passed down to consumers, and taxpayers will shoulder the costs of the courthouse.239 Perhaps it is time to divert the resources spent on this effort elsewhere. While these musings may not justify a wholesale jettisoning of civil liability on the part of breached entities, some re-thinking of liability is warranted.

C. Lessons Learned

Targeted changes to state law claims for data breach—negligence and state statutory claims such as alleged "unfair trade practices"—could perhaps better account for some of the peculiar aspects of the data breach noted above. Given that "culpability" on the part of the breached entity may often

---


236. Id.

237. See Cyrus Farivar, Target's $10M Settlement in Data Breach Lawsuit is a Tiny Price to Pay, ARS TECHNICA ONLINE (Mar. 19, 2015, 3:30 PM), http://arstechnica.com/tech-policy/2015/03/targets-10m-settlement-in-data-breach-lawsuit-is-a-tiny-price-to-pay (But for attorneys' fees and other costs related to litigation, one might question the power of data breach lawsuits to affect corporate action. A $10 million settlement offer conditionally approved in the Target case is a "miniscule amount" relative to the company's overall revenues.).

238. Goldman, supra note 182.

239. E.g., John Burnett, Smartphone industry is exposed to senseless litigation that may cost consumers, THE HILL (Nov. 5, 2014, 1:00 PM), http://thehill.com/blogs/congress-blog/technology/222718-smartphone-industry-is-exposed-to-senseless-litigation-that (discussing how litigation costs for smart phone companies are passed from the companies to the consumers).
be tenuous, liability concerning the protection of consumer personal data could be restricted to instances where a company was "grossly negligence" or "reckless." Alternatively, liability could be restricted to data breaches resulting from "insider" misconduct (e.g., hacking by an employee or consultant or the loss of equipment housing personal data) on the theory that the company has, or should have, control over the conduct of insiders, but not over cybercriminals. That the company promptly and fully complied with the applicable data breach notification statute might be an affirmative defense. Although difficult, it would be worth considering an attempt to craft some reasonable definition of causation (e.g., a specific time limit between the breach and the occurrence of harm beyond which causation is presumed to be absent).

Whether any of these issues relating to liability are pursued, a related but separate objective would remain unmet: individuals that are truly injured by a data breach should be fairly and adequately compensated. The class action model, as discussed above, does not appear well suited to accomplishing this goal; it is expensive and undercompensates the consumer victims of a breach. Two years after notice of the breach, a consumer with an uncompensated fraudulent charge of $50 is unlikely (if the results noted above are indicative) to go through the trouble of dealing with a settlement claim form, if it even arrives. The single mother with a minimum wage job whose credit rating is compromised by an identity theft will lose her apartment before the class action of which she is a member can be concluded. For the vast majority of those injured, opting-out of the slow-moving class action to pursue an individual lawsuit to seek compensation is wholly impractical because the dollar amount of the loss is too small.

A data breach compensation fund would better meet the goal of compensating true victims. It could be argued, however, that the cost of administering such a fund is just not worth the candle. Given the small percentage of persons actually victimized following a large-scale data breach, the nominal amount of monetary harm those victims actually incur, and the "self-help" mechanisms already in place so that even nominal harm might be avoided by the putative victim, is there even a need for any public compensation method? Perhaps not, but at least three reasons suggest the benefits might outweigh the cost. First, as noted above, although the median loss may be quite small, a significant number of individuals lose thousands of dollars and spend hundreds of hours remediating the theft. And for some low-wage earners or young persons, even a small loss could be significant to the family budget. Second, what the hackers will do next is anybody’s guess. Actual damage to consumers may balloon following data breaches in the near future. Having a functioning compensation scheme in place, albeit one that would have to be significantly bolstered to deal with different types of claims, might be a wise precautionary measure. Finally, some external incentive to protect consumer data, above and beyond self-interest, may well be advisable so as to discourage the cost-cutters and "bad apples" who shirk their data security
responsibilities. If properly designed, an administered compensation fund could serve this deterrent function by requiring only those companies that have engaged in specific "wrongdoing" to fund the program, while avoiding some of the objections to imposing liability discussed above.

IV. THE DATA BREACH COMPENSATION FUND

This section begins with a brief overview of administered compensation funds. Part B focuses on victim compensation funds created by statute and proposes that key characteristics of the underlying issues that strengthened the political will to enact these funds are found in personal data security breaches. This means that the creation of a data breach compensation fund, at least at the state or on a pilot basis, may be politically feasible. Part C suggests, in broad strokes, how such a fund might be designed.

A. Administered Compensation Funds

Administered compensation funds come in different flavors. Effectively, private and public insurance against the eventuality of certain losses are one type of administered compensation fund. Social welfare funds, such as Social Security and Medicare, are another type; these are funded with taxpayer dollars and administered by the federal Social Security Administration. Another example is a fund created in settlement of litigation from which payments are made pursuant to an administered payout proceeding, such as the Tobacco Litigation Settlement Fund. Another type, and the model which is proposed here, is a creature of statute, funded at least in part by private industry in exchange for immunity from or limitations on civil liability, to pay for injuries caused in whole or in part by the acts or omissions of a company.

Such an administrated system is a well recognized compensation alternative to private litigation. The benefit of an administrated compensation method over private litigation is primarily that the former can be designed to

240. E.g., Pagliery, Why Retailers Aren't Protecting You From Hackers, supra note 228.

241. See Yoo, supra note 113, at 47 (recommending a compensation fund administered by the FTC for victims of data breach, but this concept was not explored in any detail in the Yoo article).


244. E.g., Bovbjerg & Tancredi, supra note 39, at 483 ("The best known non-tort compensation method is an administrative compensation system that completely replaces tort.").
make compensation simpler and more efficient. Who and how much should be paid can be straightforward and less adversarial.

A fund can compensate more fairly than litigation. From the point of view of the victim, making a claim can be simple and inexpensive for several reasons: (1) it is relatively simple to determine whether making a claim is justified; (2) the claimant will know, in advance, within reasonable limits, what to expect; (3) claim resolution will be prompt; (4) a fund avoids the cumbersome processes and slow-turning wheels of justice dispensed through litigation; and (5) satisfaction of the claim is not dependent on external forces over which the victim has no control, such as which party has access to the best expert witnesses, or a jury’s secret deliberations. In short, an administered fund can “cover more cases, faster, more efficiently, and more predictably than tort—so as to improve compensation.”

An administered system can also be fairer to companies. Determining which companies will pay into the fund and under what circumstances can be defined in advance, eliminating the somewhat random odds that one or two in a sector will be named in a lawsuit, while others—equally blameworthy—

245. For one thing, if payment is made on a “no-fault” basis, the entire liability phase of a trial is omitted, and there would be little or no need for any evidence regarding the events leading up to the data breach. See Janet Cooper Alexander, Procedural Design and Terror Victim Compensation, 53 DePaul L. Rev. 627, 645 (2003) (discussing the procedural design of the 9/11 Victims’ Compensation Fund); Betsy J. Grey, Homeland Security and Federal Relief: A Proposal for a Permanent Compensation System for Domestic Terrorist Victims, 9 N.Y.U. J. Legis. & Pol’y 663, 720 (2006) (An administered fund “saves litigation costs for both plaintiffs and defendants, avoids duplicate litigation of identical or nearly identical issues, and reduces the burden on the judicial system.”).

246. See Elizabeth C. Scott, The National Childhood Vaccine Injury Act Turns Fifteen, 56 Food & Drug L.J. 351, 362 (2001) (though the defendant’s antagonistic positioning has been removed from the process, some adversity may remain, as between the administrators, who must appropriately distribute a limit fund, and claimants).

247. E.g., Grey, supra note 245, at 669.


249. See Alexander, supra note 245, at 648 (“By contrast, tort plaintiffs must prove liability, bear the risk that the jury may find against them in the liability phase, pay attorneys fees from any recovery (unless unusual circumstances permit fee-shifting), and enforce the judgment.”).

250. See id.

251. Bovbjerg & Tancredi, supra note 39, at 483.
are spared. Compensation awards, and therefore business costs, can be more reliably predicted.

Because of the advantages, administered compensation funds have been proposed as a replacement to litigation that arises from medical malpractice, defective products, and terrorism to name but a few. However, few of these proposals are enacted, at least not on a large scale. The reasons some proposals fail are no doubt many, complex, and overlapping. Yet the same is ostensibly true for those proposals that are adopted. In other words, as summarized below, some of the better-known statutory funds appear to address vastly different kinds of victims and injuries, offer immunity from civil litigation to different industries for different reasons, and have sprung from differing political climates. A closer comparison of these funds reveals common underlying features that are perhaps shared with data breach victims, however, and that are analogous to the causes and consequences of data breach.

B. The Victims' Compensation Fund

Workers' compensation is the “three hundred pound gorilla” amongst victims' compensation funds. In very brief summary, early in the twentieth century, a “rising tide” of concern arose over the disturbing increase in the number of injured and disabled workers consequent to the industrial revolution. Factory work was dangerous, and many were injured. Increasingly, injured employees sought compensation through private litigation, which brought a measure of relief to a limited number of individuals. But the outcomes were unpredictable; employees suffered inadequate measure of compensation, and employers, likewise, faced uncertain threats of liability from which they advocated relief. From this, the “historic compromise”


254. See generally, Grey, supra note 245, at 719.

255. See, e.g., Virginia Birth-Related Neurological Injury Compensation Act, VA. CODE ANN. §§ 38.2-5000–5021 (West 2016) (exemplifies the more common approach of establishing a compensation fund for a selected sub-class of injuries or injured persons).


257. See id. at 163.

258. See id. at 167.
was born.259 States enacted workers' compensation legislation requiring employers to purchase insurance to cover employee claims; generally, employee claims for unintentional injuries incurred on the job would be paid regardless of fault, and general immunity from civil liability would be granted to employers.260

Similarly, the National Childhood Vaccination Compensation Fund (NCVCF),261 enacted in 1986, created a mandatory no-fault compensation system for persons injured through childhood vaccines.262 Although the widespread administration of vaccinations against many childhood diseases (e.g., whooping cough, diphtheria, tetanus, and others) had been "spectacularly effective" in improving public health,263 in rare cases, these vaccines caused injury, and even death.264 Faced with an increasing number of lawsuits,265 some of the vaccine manufacturers ceased production. As a result, the NCVCF was established to ensure the availability of the life-saving vaccinations.266 The NCVCF is funded by a surcharge on exported pharmaceuticals, and while it limits, it does not eliminate liability.267 To make a claim, a victim must first apply to the fund administrator; if unsatisfied, the victim may then appeal to the courts where some deference will be given to the fund administrator.268

The 9/11 Victims Compensation Fund moved quickly through Congress, as the nation was eager to show support and compassion for the victims of the terrorist attack, and legislators had become convinced of the wisdom of limiting the liability of the airline carriers who were already reeling from a reduction in airplane travel following the attacks.269 The airline industry provided a significant portion of the funds (though taxpayers also contributed) in exchange for restrictions on liability to the victim: victims could apply for compensation through the fund or choose to go to court, but

259. Id. at 168.
262. See Schwartz & Mahshigian, supra note 248, at 387.
263. Id. at 388.
264. See id.
265. See Scott, supra note 246, at 355 ("Plaintiffs were filing over 100 new cases annually, requesting damages of over $ 3.5 billion, and manufacturers were struggling to pay damages and defense costs.").
266. See id.
267. See id. at 356–57.
268. See id. at 362.
if the latter was chosen, the statute capped liability to the amount of the defending carrier's insurance coverage.\(^{270}\)

One thing disparate funds seem to have in common is a characteristic of the victims: their harms were unexpected and were not a result of their own actions. This essential “victimhood” justifies special efforts to ensure that these individuals receive efficient and fair compensation. The unfortunate few include victims of injury in the workplace; families and children suffering from the effects of childhood vaccination; those who died in the South Tower; and the emergency responders potentially exposed to disease as a necessary consequence of their jobs. At the time workers' compensation statutes were enacted, workplace injuries were considered “necessary exigen-
cies” of one’s daily occupation, over which one had no control, such that it would be unjust for those workers to bear the burden.\(^{271}\) Most children have to be vaccinated in order to attend public school,\(^{272}\) and because “state gov-
ernments require children to undergo a risk in order to protect society as a whole,” Congress found it appropriate to create “a national fund to com-
pensate children who are injured because of these risks.”\(^{273}\) The victims of 9/11 “were believed to have died on behalf of all Americans, creating a justifiable, communitarian sense that the loss should not fall disproportionately on those who were unfortunate enough to occupy the targets at the fatal moment.”\(^{274}\) By way of contrast, an individual has at least some measure of control in deciding whether to have a medical procedure and a choice in the provider. Similarly, an individual can choose to purchase a Ford or a GM car, or forego an automobile in favor of public transportation. While some victims are—fairly or unfairly—labeled mere money-seekers by tort reformers,\(^{275}\) it is not easy to characterize the victims of 9/11 in the same manner. Nor is it palatable to leave the entire cost of their injuries on those few children who reacted poorly to vaccines, when those vaccinations have benefitted all of society by creating “herd immunity.”\(^{276}\)

\(^{270}\. \) Id. at 143, 145.

\(^{271}\. \) Spieler, supra note 256, at 165–66 (quoting Theodore Roosevelt).

\(^{272}\. \) Schwartz & Mahshigian, supra note 248, at 393. In most states an exception will be made for a religious or “personal” objection by the parents, though these exclusions are currently under fire; see Vaccine Laws, NAT'L VACCINE INFO. CTR., http://www.nvic.org/vaccine-laws.aspx (last visited Jun. 2, 2016).

\(^{273}\. \) Schwartz & Mahshigian, supra note 248, at 393.

\(^{274}\. \) Ackerman, supra note 269, at 159.

\(^{275}\. \) Id. at 158 (discussing the characterization of tort reformers).

\(^{276}\. \) Scott, supra note 246, at 359 (“The notion of herd immunity, in which society bears the cost of vaccine injuries because compulsory immunization lessens the risk that the disease can be introduced and harm members of the community, is given as one of the major reasons why society, and not manufacturers, should be responsible for injuries incurred when vaccines are administered.”).
Related to the notion of “true victimhood” is the fact that while many people were in harm’s way, only a few were harmed. For example, although millions of children have received vaccinations, only a very small number were seriously injured. In addition, 9/11 was considered a terrorist attack on America; the unlucky few were the Americans who died or were injured. The perception that “we are all in this together” could have been a factor in mobilizing political support for these funds.

A second common factor is that these compensation funds protect putative defendants from civil liability from “wrongful” acts or omissions when the primary causative agent was a force, largely or entirely, out of the defendants’ control. During the height of the Industrial Revolution, when workers’ compensation statutes were enacted, “[i]ndustrial carnage was almost universally viewed as an inevitable, albeit unfortunate, consequence of modern industrial enterprise.” The grinding machinery, not the employer, was the primary cause of injury, but one that had to be endured to turn the wheels of commerce. The vaccines that saved so many children’s lives posed an “unavoidable” risk of harm to a few, due to the characteristics of the organisms comprising the vaccine, not a design or manufacturing defect. The airlines whose planes were hijacked on 9/11 may have been secondarily liable for negligence, but it was the awful acts of terrorism that loomed in peoples’ minds. Otherwise stated, the injuries to the individual victims might have been preventable, but at an inordinate cost.

Finally, in each of these programs there is a clear “triggering” event for distribution from the fund. With documentation showing the administration of a vaccination within a specified period prior to the onset of symptoms, a claim can be made to the NCVCF. Eligible claimants for compensation from the 9/11 Victims Compensation Fund were persons at the World Trade Center, the Pentagon, or Shanksville, Pennsylvania at the time, or in the immediate aftermath, of the plane crashes. A triggering event may

277. See id. at 352 (reporting that in 1997 coverage among children exceeded 90% for the DPT vaccine).
278. Id. at 353.
279. Ackerman, supra note 269, at 159.
280. See id.
281. Spieler, supra note 256, at 164.
282. Since the turn of the twentieth century, society’s acceptance of this “inevitability” has changed considerably, and employers are expected to provide a reasonably safe environment for employees. See id. at 162–64.
283. See Schwartz & Mahshigian, supra note 248, at 388.
284. See id. at 396 (contrasting the NCVCF with contemporaneous proposals to establish a compensation fund for consumers injured by defective products).
286. Ackerman, supra note 269, at 160.
not seem, at first blush, to be a characteristic of employees injured on the job: the number of direct causes of injury is probably close to infinite. But from a bird’s-eye view, there is a universal, indirect cause. All were injured because of their employment, and that is a sufficient cause—no more precise cause need be identified—to entitle the employee to seek compensation. Although the employee may not be able to establish that the injury was a consequence of employment rather than a result of any intentional misconduct, ultimately, eligibility to seek workers’ compensation depends only on that one element: employment.

These three underlying features of established compensation funds can also be discerned in the background of data breaches. In terms of true “victimhood,” individual consumers have had no real ability to prevent a breach of their personal information. A handful of Americans may be able to conduct their lives without the use of any transaction in which digitized personal identification is exchanged for goods and services, but there are not many of those folks. This also means that the potential risk of harm from compromised data is virtually universal. We are, indeed, in this together.

In terms of culpability, when a company’s data, including the personal information of the company’s customers or clients, has been hacked, the primary liability rests with the unknown thief. The company could be held secondarily liable for the theft but, as discussed above, there are many reasons to be extremely judicious in defining “fault.” Otherwise stated, these reasons might justify a “pressure release mechanism” in the form of a no-fault, administered claims procedure as an alternative or pre-condition to civil liability.

And finally, the “triggering” event can be readily defined; the compromise of personal data by an actor outside the immediate control of the breached entity. Thus, it may be politically feasible to explore the possibility of creating a data breach victims’ compensation fund.

287. See generally supra Part II.B.1.


289. Presumably, as with the data breach notification statutes, these efforts would begin in the states. A national fund may at some point be preferable, given the national reach and/or data interconnectedness of business today. See generally Peters, supra note 13. But this seems improbable in the foreseeable future given the general political polarization in the Federal Congress during this era, and its demonstrated failure to pass any significant data security legislation over the past decade. And a state-based solution does have advantages: smaller scale, more flexibility, and different models can be tried, compared, and revised.
C. A Data Breach Victims Compensation Fund

Many potential issues exist in designing a compensation fund. Such issues range from the fund’s structural composition, such as how the program will be administered and by whom, to eligibility, claims procedures, measure of damages, and the process for review of awards. The discussion below is limited to the two primary objectives of a compensation fund—limiting liability, and providing expeditious and fair compensation—and proposes how one might best accomplish those two objectives.

The data breach victims’ compensation fund should be a no-fault alternative to remedies based on state tort claims, breach of contract, and consumer protection statutes. The compensation fund would require individual data breach victims to file a claim with the fund before filing a lawsuit directly against the breached entity; the victim would be free to pursue a lawsuit directly against the hacker. An alternative to this pure “exhaustion” requirement is to give victims the option of making a claim or proceeding directly to court. This design functions, at least partially, to ensure that the fund is not a “get-out-of-jail free” card for those companies who do not implement reasonable security measures. But this design is only feasible when a finite number of potential victims arising from a singular occurrence exist, or a limited number of incidents exist, because if the events giving rise to harm are ongoing, giving victims this option leaves the courthouse door wide open to class action and other lawsuits; this would defeat the purpose of the fund.

A better solution would be to identify those companies whose data breaches were most preventable, as defined below, and tax these with funding the program; this would incorporate both pure no-fault as a basis for compensation and a penalty for some measure of fault. At this time, the tax should not create an inordinate financial burden for the companies. Based on

290. Alexander, supra note 245, at 662.
291. See id.
292. See id. at 683.
293. Id. at 671 (“. . . the compensation program is a substitute for tort litigation against the protected entities, but not others.”) This exclusion might have little practical consequence, but there would surely be instances in which a hacker claimed responsibility or was caught by the authorities and was subject to service of process.
294. Conk, supra note 288, at 220.
295. See id. at 252.
296. See id. at 253–54.
297. See id. at 255–58.
298. See id. at 258.
299. See id. at 197–98, 259.
the available data on the number of persons who incur a direct loss on account of a data breach, and the average amount of that loss, the total amount needed to fund the program should be reasonably modest, even if all injured parties actually filed a claim, which seems highly unlikely. It would be an additional cost to the compensation fund or taxpayers if public investigators were designated to evaluate large-scale breaches to determine whether the breached entity should be subject to this fund tax. However, public investigation would be limited, because data breach notification statutes require companies to disclose the breach. There would be no need, therefore, to determine whether a crime had occurred, a regulation had been violated, or to ascertain the identity of the culprit. If the notification statutes were to require sufficient detail about the circumstances of the breach, costs could be reduced by further streamlining investigations.

To facilitate investigations intended to determine whether a fund tax is owed, and to avoid the unfairness of imposing liability “wholesale” discussed above, liability could be limited to pre-determined “avoidable classes of events.” Specifically, a breach caused by an act or omission of the company housing the data that caused a highly-preventable breach (taking into account the costs of protecting against breach, available technologies, the nature of the industry, etc., as agreed by data security experts) would give rise to a fine to be paid into the fund. Alternatively, or in addition, fines from civil actions taken by state authorities against companies that fail to comply with data breach notification statutes could also be dedicated to the compensation fund.

300. Conk, supra note 288, at 259; see also discussion supra Part II.B.1.
301. See discussion supra Part III.A.
303. See First-of-its-kind lawsuit for unnecessary delay in data breach notices, supra note 302.
304. See id.
305. See id. The California data breach notification may come closest to meeting this objective. Most such states’ statutes would, however, as currently written, not provide sufficient information. See Pagliery, Why Retailers Aren’t Protecting You From Hackers, supra note 228.
306. See discussion supra Part II.B.1.
308. See id. at 482 (defining “ACE’s” in the context of medical malpractice).
309. See First-of-its-kind lawsuit for unnecessary delay in data breach notices, supra note 302.
The question of eligibility should be straightforward. Anyone would be eligible to file a claim as long as their personally identifiable digital data has been compromised by a hacking incident into the computers or networks of an entity that regularly collects and houses that data for ordinary business purposes. The notice provided by that entity pursuant to a data breach notification statute would substantiate eligibility. Those persons living in the three states without such legislation who are the victims of breach might turn to one of the number of private services that compile publicly available lists of data breaches.

It is proposed that only out-of-pocket losses should be compensable, which include non-reimbursed fraudulent debit or credit transactions or other direct charges, any actual costs incurred in replacing cards or contacting service providers to change account information, and documented time spent repairing the consequences of the data compromise with a set hourly rate and upper limit on the number of hours that could be claimed. Only costs directly associated with the breach should be compensable. Thus, mitigation expenses, such as the purchase of a credit monitoring service, would not be compensated, since these costs are voluntarily assumed by the data breach victim. Including these as compensable damages would inordinately increase the complexity and cost of administering the fund: more documentation would have to be collected and more judgments would have to be made about the validity and reasonableness of the amount claimed. In addition, given the other mitigation measures already in place and the fact that the chance of being an actual victim as a result of a large-scale breach is quite small, incurring the cost of credit monitoring services is basically a wild "shot in the dark," and not a reasonable expense that should be compensated.

Alleged injury from future harm, such as an increased risk of identity theft, should not be compensable. First, any method of setting a "dollars and cents" amount to such a claim would be no better than a wild guess. Second, and again, it is not very likely that the "future harm" will ever actually come to pass. Finally, if an individual's personal information is misused sometime in the future (presumably some significant period of time after the breach for which compensation is sought) then it is entirely possible that the information was stolen from another source.

As for "emotional distress" resulting from the data compromise itself, this alleged injury should ordinarily not be compensable from the fund. This follows from the evaluation of this type of injury in the law of torts. Not just any slight or hurt, unaccompanied by physical harm, is a compensable event. Instead, there must be shown the existence of "severe emotional distress" caused by truly outrageous conduct. Certainly hacking is a crime, and it may surely be considered despicable and underhanded, but "outrageous"? One

310. Whether or not these should confer legal standing is a separate issue not addressed in this article.
311. See Remijas v. Neiman Marcus Grp., 794 F.3d 688, 692–93 (7th Cir. 2015) (showing injuries commonly alleged by data breach plaintiffs).
would think ordinarily not. On the other side of the equation, one could imagine limited exceptions, but the threat of a loss of $99 would surely not cause the ordinary person "severe emotional distress."

Thus set, the parameters for compensation from the fund would largely parallel those that are often part of the terms of a litigation settlement agreement: out-of-pocket losses directly caused by the breach are compensable.312 This, it seems, just makes sense: the compensation fund would be, in effect, a generalized "settlement agreement" between consumers and the industries that house their personal information.

V. CONCLUSION

It is unsettling to receive notice that one's personal information has been stolen from the local "big box" store by a hacker, or to read about a massive data breach in the newspaper and realize the breached insurance company is one's carrier. It is bothersome to contact Amazon and Netflix to change credit account information. But for most individuals whose basic personal information has been compromised by a breach, empirical data suggests that little to no real injury results.313 Still, victims should not be forgotten because they lack the sophistication, or fail to take reasonable precautions to protect their own data. These victims spend hours untangling the mess or lose precious money from their bank accounts. But using the sledgehammer of class action lawsuits against the breached entity seems quite unnecessary in terms of fairly and efficiently providing compensation to the individual victims of the breach. By way of analogy, in the world of torts, it is black-letter law that only "outrageous" conduct that causes extraordinary distress supports a claim for intentional infliction of emotional distress; people are expected to endure the "ordinary" slings and arrows shot by others, even if some emotional harm is caused. Perhaps the same should be true for the "ordinary" breach by hacking of the local retailer or insurance company.

Far more pressing as an objective than compensating individual victims, it would seem, is stopping the hacking. Leaving aside the importance of securing highly-classified national security information, one's personal data is an expanding and increasingly rich target as more and more types of personal data are collected (on wearable activity and performance enhancement devices, home appliance monitors, and various apps for everything, to name but a few). If not now, soon, it would seem, a data thief could truly steal a per-

312. Any equitable remedies incorporated in such agreements would, however, be unavailable. These types of remedies would remain the province of regulatory agencies, or would perhaps be voluntarily undertaken by the breached entity to forestall the possibility of another costly breach. See, e.g., In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 851 F. Supp. 2d 1040, 1049 (S.D. Tex. 2012).

313. This could change, of course: the next generation of hackers may devise new ways to extract more from their ill-gotten data gains, and cause individual victims greater injury.
son's identity, not just a name, address, and credit card number. If private civil lawsuits based on the existing common law and consumer protection statutory causes of action were an effective tool for achieving the goal of data security, these claims should by all means be encouraged. But there are certainly good reasons to question whether this is so and to consider other ways to ensure that the companies that collect our data take all necessary and reasonable measures to protect that data from thieves.