Needing A New Approach to Address Employee Data Breaches in the American Workplace

Jeremy Barbanell*

ABSTRACT

The Sony Pictures Entertainment data breach of 2014 dramatically illustrated the risk of identity theft that workplace data breaches pose to American employers' employees. Recognition of that risk occurred as long ago as 2003. Many if not most data breaches have gone undetected since as long ago as 1996—and that may always be the case. In other words, the reality has been and may always be that often (1) employees know that their personal data has been compromised only when they become victims of identity theft, and (2) employees do not know that their employers are the source of the breached data.

For those and other reasons, the current remedies those employees are expected to use to address data breaches—i.e., breach notifications, ex post defensive efforts, and lawsuits—are inadequate. The need for a new remedy is clear.

This paper presents a novel analysis of the inadequacies and need noted above by proposing how the need might be satisfied. It also evaluates the proposal in relation to data breaches, workers' compensation laws, and employer-provided health insurance in the United States of America. In doing so, this paper also notes how the adoption of the proposal might enable a potentially new means of detecting data breaches.

INTRODUCTION

On November 24, 2014, a disturbing image appeared on the screens of devices being used by Sony Pictures Entertainment ("Sony's") employees to try to access their workplace network. It was a picture of a stylized, red-hued human skeleton reaching toward them. The expressive shaping of the sockets housing its sunken eyes, and the pointed teeth lining its open mouth, gave it a menacing appearance. Situated before the skeleton was a message stating that all of Sony's internal data had been stolen.[1]

In the weeks thereafter, thousands of people—current and former Sony employees—had the following kinds of information about them posted online: names, social security numbers, birth dates, home addresses, medical information, tax records, job titles, performance evaluations, scans of passports and visas, salaries, bonus plans, reasons for termination, and details of severance packages.[2] Sony employees then received emails, allegedly from the parties responsible for releasing the information, which threatened harm to them and

---

* Jeremy Barbanell is a third-year law student at the University of San Diego School of Law. This paper is dedicated to my family. For help with editing, thanks goes to Jessica Olsen, Rachel Bolling, Jessica Olsen and Charles Quarto. For providing me with valuable insights, thanks goes to Professors Richard Paul and Sharmila Sohoni.
Thanks also goes to Rishi Bhatt, Jacob Corirossi, John Eichelberger, Nicholas Quarto and Pinhas Rahav.

[1] Plaintiffs' Complaint 7, Michael Corona and Christina Mathis v. Sony Pictures Entertainment, Inc. (C.D.Cal.) (No. 2:14-cv-09600), *available at* http://www.jdsupra.com/post/fileServer.aspx?fName=cc00c1a8-694a-489f-a1ce-78141bc8568a.pdf .

[2] *Id. at* 7-9, 31-32.

their families.[3]

This was not the first time that the private data of a company's employees was made public by a data breach:[4] more than a decade before, an article published in USA Today noted that such incidents were occurring.[5] However, the Sony breach appears to have been unprecedented for two reasons. First, there were explicit threats made against the employees. Second, the employees brought a class action lawsuit against their employer. Given these elements, questions about the legal duties of employers to protect stored information about their employees have been raised anew.

In approaching these matters, many have focused on three areas. The first is increasing protection of data. The second is notifying those whose information has been exposed by breaches. The third is litigation brought by victims of data breaches against those whose databases, containing the victims' information, were breached. All those approaches have some merit. Yet, they are at least *presently* inadequate for serving as the only sources of protection or justice for employees in the aftermath of data breaches. They are also inadequate because they do not reflect an appreciation of certain facts, particularly the fact that it has been suggested, for at least nearly two

---

[3] *Id. at* 10.

[4] A "data breach" occurs when your confidential information is released without your control or permission, but does not always lead to identity theft." RONALD J. LEACH, IDENTITY THEFT IN THE CYBER AGE 7 (AfterMath 2012).

[5] Stephanie Armour, *Employment Records Prove Ripe Source for Identity Theft,* USA TODAY (Jan. 23, 2003), *available at* http://usatoday30.usatoday.com/money/workplace/2003-01-23-idtheft-cover_x.htm (last visited Apr. 24, 2015).

decades, that most data breaches go undetected.[6]

The sources of justice for employees in the aftermath of data breaches must be radically augmented to reflect such realities. This paper, so far as can be determined, is novel in recognizing that and proposing how it might be done. Part II summarizes background information relevant to data breaches, and discussions of data breaches in subsequent parts of this paper. The current policies in place to provide for employees in the aftermath of data breaches are presented and analyzed in Part III. A new approach with which employers might (1) better tend to the well-being of their employees in the aftermath of workplace data breaches involving employees' personal information, and (2) detect such breaches, is presented in Part IV. The approach is explored directly, but also indirectly, via examination of methods of dealing with surprisingly similar matters—like employer-based health insurance and workers' compensation. Part V concludes this analysis.

I. BACKGROUND INFORMATION ABOUT DATA BREACHES

According to the Internal Revenue Service, "[i]t is almost impossible to be in business and not collect or hold personally identifying information — names and addresses, Social Security numbers, etc., about your customers, employees or patients."[7]

---

[6] *Infra* note 16, 17, 18, 19, 20 and accompanying text.

[7] INTERNAL REVENUE SERV., HAS YOUR BUSINESS BECOME THE VICTIM OF A DATA SECURITY BREACH? (2014), http://1.usa.gov/1PB5acD; *see also* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 256 (2005) ("A myriad of entities—

For that reason, and at least two others, small businesses[8] have been the primary victims of data breaches[9]. The other two reasons are that (1) many small business owners cannot afford to fight off breaches,[10] and (2) the vast majority of businesses

---

including businesses, non-profit organizations, and the government—assemble…masses of computerized information relating to individuals. The data often includes—but is not limited to—names, relationships (e.g., family members and employers), contact information (e.g., phone numbers, residences, and virtual addresses), personal histories (e.g., birth dates, medical data, physical characteristics, and educational records), official identifiers (e.g., social security, driver's license, and passport numbers), and financial records (e.g., bank, credit card, frequent flyer, and investment account numbers).").

[8] The U.S. Small Business Association defines small businesses as businesses with fewer than 500 employees, and 99 percent of all independent enterprises in the United States of America match that description. Pamela S., *The Shocking Truth About Small Business: Data Security is on the Back Burner*, IPOST (Jan. 23, 2013), http://bit.ly/1F0L5d2.

[9] Cheryl Conner, *Are You Prepared? Record Number Of Cyber Attacks Target Small Business*, FORBES (Sept. 14, 2013), *available at* http://onforb.es/18lFIDb ("The 2012 Data Breach Investigations Study by Verizon shows that in 855 data breaches they examined, 71 percent occurred in businesses with fewer than 100 employees. Verizon's 2013 Report shows attacks on small business increasing in record numbers as well."), *citing* VERIZON BUSINESS, 2012 DATA BREACH INVESTIGATIONS REPORT (2012), http://vz.to/1lvQNI4.

[10] *Top 8 Data Breach Misconceptions*, INSUREON (Jan. 12, 2015), http://www.insureon.com/blog/post/2015/ 01/12/top-8-data-breach-misconceptions.aspx; Robert Vander Meiden, *Can Small Businesses afford Managed IT Services?*, COMTECH (Feb. 27, 2015), http://www.comtech-networking.com/blog/item/128-can-small-businesses-afford-managed-it-services; John Brandon, *Why Your Business Might Be a Perfect Target for Hackers*, INC. (Dec. 2013-Jan. 2014), *available at* http://bit.ly/1bpp0CM ("put in place the

are small ones.[11] In contrast, as was noted in a story broadcast by CBS's *60 Minutes* in 2014, "'Most of the large companies are growing their security spending. Yet[,]… 97 percent of all companies — are getting breached.'"[12] Last year alone, 43 percent of companies experienced a data breach.[13]

This increase in data breach occurrence seems to be the product of a steadily and continuously degrading situation.[14] It has developed over a period of years in which *detected* data

---

best tech barriers you can afford"); Max Knoblauch, *78% of Organizations Experienced a Data Breach in the Past 2 Years*, MASHABLE (Apr. 15, 2014), http://on.mash.to/1n8HcvI [hereinafter, Knoblauch, *78% of Organizations*] ("Money is likely the biggest factor in a lack of data security. In a 2013 survey by the National Small Business Association, 44 percent of small business owners cited the cost of upgrading technology as one of their biggest challenges."), *citing*, *2013 Small Business Technology Survey*, NAT'L SMALL BUS. ASS'N (Sept. 16, 2013), *available at* http://bit.ly/19Ab3rw.

[11] *Supra* note 8.

[12] *60 Minutes Story Claims 97 Percent of Businesses Have Already Been Hack*ed, ACE IT SOLUTIONS (Dec. 1, 2014), http://bit.ly/1AQ53TU, *citing* Bill Whitaker, *What Happens When You Swipe Your Card?*, CBS NEWS (Nov. 30, 2014), *available at* http://cbsn.ws/1v8t7SH.

[13] Elizabeth Weise, *43% of Companies Had A Data Breach in the Past Year*, USA TODAY (Sept. 24, 2014), http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/.

[14] As one author wrote, "If it sometimes appears that just about every company is getting hacked these days, that's because they are." Jaikumar Vijayan, *90% of Companies Say They've Been Hacked: Survey*, COMPUTERWORLD (June 20, 2011), http://www.computerworld.com/article/2509366/security0/90--of-companies-say-they-ve-been-hacked--survey.html, *citing Perceptions About Network Security*, PONEMON INST. (June 2011), http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf.

breaches have dramatically increased in frequency and size.[15] Yet, The exact source of information revealed by a data breach—e.g., a breach of *Sony's* systems—is often unknown, as of 2014 up to 85 percent of data breaches suffered by companies went undetected,[16] and the same might be true of up to 40 percent of data breaches involving the federal government.[17]

The fact that "[u]ndoubtedly[,] a large number of breaches and attempt[ed data breaches] go undetected,"[18] is striking. So too is the fact that most data breaches were recognized as going undetected at least as long ago as 1996, again in

---

[15] *Year of Mega Breaches & Identity Theft*, BREACH LEVEL INDEX 14 (2014), http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf [hereinafter, BREACH LEVEL INDEX, *Mega Breaches*]; *see also* George V. Hulme, *Cybersecurity 2014: Breaches and Costs Rise, Confidence and Budgets Are Low*, CSO (Nov. 5, 2014), http://bit.ly/1tdrz3F (noting that since 2009, "annual growth rate of detected incidents has risen 66 percent").

[16] Eric Vanderburg, *Organizations Are Failing At Early Breach Detection*, JURINNOV, http://bit.ly/1cGoitM (last visited May 8, 2015) [hereafter, Vanderbury, *Early Breach Detection*], *citing* Oliver Rochford & Kelly M. Kavanagh, *Using SIEM for Targeted Attack Detection*, GARTNER (Mar. 12, 2014), http://gtnr.it/1zRrMnw; *see also* Megan Leonhardt *Cybersecurity Breaches Not Rare, Just Undetected*, WEALTH MGMT. (Sept. 13, 2014), *available at*, http://bit.ly/1pTxjOt [hereafter, Leonhardt, *Not Rare, Just Undetected*].

[17] MINORITY STAFF OF THE HOMELAND SEC. & GOVERNMENTAL AFFAIRS COMM., THE FEDERAL GOVERNMENT'S TRACK RECORD ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE (Feb. 4, 2014), *available at* http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A.

[18] Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 360 (2006), *available at* http://ir.lawnet.fordham.edu/flr/vol75/iss1/9.

1999 and 2006,[19] and yet again in 2014.[20] A significant reason for this lack of detection is that, "[c]riminals go to great lengths to make sure breaches go undetected,"[21] and many or most data breaches are caused by employees.[22] It can be argued, though, that employees are often able to cause the breaches due to inadequate security measures taken by their employers.[23]

---

[19] *Id.* at 360, *citing* Kevin J. Soo Hoo, *How Much Is Enough? A Risk-Management Approach to Computer Security*, STANFORD U. CENTER FOR INT'L SECURITY & COOPERATION 30 (Aug. 2000), *available at* http://cisac.fsi.stanford.edu/sites/default/files/soohoo.pdf (citing a Defense Information Systems Agency report from 1996 which, based upon "a very large simulation/red-teaming exercise that utilizes publicly available 'hacking' algorithms and tools to attempt to breach the computer security of Department of Defense information systems," estimated that "96 percent of the successful break-ins were undetected"); Mike Burkitt, *The Failure of the Traditional Firewall*, COMPUTERWEEKLY.COM (July 1999), www.computerweekly.com/feature/The-failure-of-the-traditional-firewall ("In perhaps the most frightening statistic of all, the FBI and CSI estimated last year that as many as 97 percent of all computer security breaches today go completely undetected.")

[20] *Supra* notes 16-17 and accompanying text.

[21] CISCO, CISCO 2014 ANNUAL SECURITY REPORT 36 (2014), http://bit.ly/VNp53a.

[22] *Compare* Robert Siciliano, *Data Breaches: How to Protect Your Business From Internal Threats*, HUFFINGTON POST (July 20, 2014) http://www.huffingtonpost.com/robert-siciliano/data-breaches-how-to-prot_b_5357354 .html, *citing* Heidi Shey et al., *Understand the State of Data Security and Privacy: 2013 to 2014*, FORRESTER (October 1, 2013), http://bit.ly/1dWig8O (employees are the cause of most breaches) *with infra* note 23 (employees are the cause of many, but not most, breaches).

[23] *See*, *OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented*, ONLINE TRUST ALLIANCE (Jan. 21, 2015), http://bit.ly/1J7NiF5.

Given this state of affairs, it is perhaps unsurprising that some have suggested that it is impossible, possibly impossible, or nearly impossible to stop all data breaches.[24] This is alarming given that most businesses are small business, and 80 percent of small businesses suffering data breaches declare bankruptcy or suffer severe financial losses within two years of the breaches.[25] It is even more alarming given the increasing threat this seems to pose to people connected with these businesses, such as employees.

To better appreciate this increasing threat, one must understand in greater detail than has been

---

[24] Afrah Fathima & Badiuddin Ahmed, *Making Data Breach Prevention a Matter of Policy in Corporate Governance*, 2 INT'L J. OF SCI. ENGINEERING & TECH. 1, 6 (Jan. 1, 2013), *available at* http://bit.ly/1cGqBgy; Matt Chandler, *Repercussions of a Data Breach Can Be Disastrous*, BUFFALO L. J. (July 15, 2013), *available at* http://www.bizjournals.com/buffalo/blog/buffalo-law-journal/2013/07/repercussions-of-a-data-breach-can-be.html?page=all; Kathryn Small, *Data Breaches Caused By Human Error, Hardware Theft*, IT NEWS (Oct. 21, 2008), http://www.itnews.com.au/News/126104,data-breaches-caused-by-human-error-hardware-theft.aspx; Taylor Armerding, *Needed: Breach Detection Correction*, CSO (May 27, 2014), http://bit.ly/1dWi3T7.

[25] *Supra,* note 8 (Most businesses are small businesses); Dan Ryan et al., *The Cyber War Against Small and Medium-Sized Businesses*, INLAND EMPIRE BUS. J. 40 (Sept. 2013), *available at* http://bit.ly/1GZnPue; Knoblauch, *78% of Organizations*, *supra* note 10; *see also*, Max Schleicher, *The Data Breach Statistics Nobody is Talking About*, TECHINSURANCE (Oct. 25, 2013), http://www.techinsurance.com/blog/cyber-liability/data-breach-statistics-nobody-is-talking-about/ [hereinafter, Schleicher, *Data Breach Statistics*] (significant losses stem from lawsuits and payment of damages).

provided above the ways in which data breaches have changed over the years. Between 2005 and 2013, the number of reported data breaches increased by 300 percent.[26] Compared to previous years, "[m]any of the breaches in 2014 involved the theft or compromise of…information, such as names, addresses and Social Security numbers."[27] This is very troubling for two reasons. First, if one's data was stolen in 2011, one only had a 10 percent chance of becoming a victim of identity theft. In 2014, a third of people affected by data breaches became victims of identity theft.[28] The significance of the increased probability of identity theft seems amplified when one recognizes, as perhaps many do not, the following. Identity theft "goes well beyond stealing and using someone's credit card or taking out credit cards in someone's name." [29] As one source puts it:

> [C]riminals [may] use the…identity to obtain a driver's license and… [otherwise] commit fraud… In these cases, [fixing] the situation requires…more than…canceling credit

---

[26] Amrita Jayakumar, *Cyberattacks Are On the Rise, and Health-Care Data is the Biggest Target*, WASH. POST (Feb. 5, 2014), *available at* http://wapo.st/1c42Szk ("But there's no doubt the number of data breaches across sectors has increased. Since…2005, the number of reported breaches is up nearly 300 percent. In 2013 alone, the number of breaches was 30 percent higher than in 2012. And the leading cause of stolen data last year was hackers.").

[27] BREACH LEVEL INDEX, *Mega Breaches*, *supra* note 15.

[28] Kathy Kristof, *Fraud Risk Soaring For Data Breach Victims*, CBS NEWS (Feb. 5, 2014), http://cbsn.ws/1e6hMVv.

[29] Joanne Sammer, *Identity Theft Protection as an Employee Benefit*, SOC'Y FOR HUM. RESOURCE MGMT. (July 16, 2008), http://bit.ly/1IsvEOR [hereinafter, Sammer, *Identity Theft*].

> cards and opening new accounts. There are lasting effects of identity theft… [V]ictims are often harassed by debt collectors, denied new credit, unable to use existing credit cards…, have their utilities cut off, are subjected to a criminal investigation or civil suit, and have difficulties obtaining or accessing bank accounts. In some cases…victims are arrested if someone committed a crime and used [their] identity when providing information to law enforcement officials.[30]

In 2012, the Bureau of Justice Statistics issued a report revealing how much identity theft can cost its victims in terms of time and money. It found half of identity theft victims spent a day or less resolving problems related to the crime, but 29 percent of victims spent a month or more.[31] While 14 percent of victims suffered out-of-pocket financial losses when counting only direct losses,[32] when counting indirect losses,[33] that number

---

[30] *Id.*

[31] Erika Harrell, *Victims of Identity Theft, 2012*, *in* BUREAU OF JUSTICE STATISTICS BULLETIN 10 (2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

[32] Alexander Trowbridge, *Identity Theft Rises, Consumers Rage*, CBS NEWS (July 1, 2014), http://www.cbsnews.com /news/identity-theft-rises-consumers-rage/. "Direct losses" refer to "the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained." *Supra* note 31 at 6.

[33] Indirect losses include "legal fees, bounced checks, and other miscellaneous expenses (e.g., postage, phone calls, or notary fees)." *Supra* note 31 at 6. Another source defines them as including, "lost wages, lawyers' fees, higher interest rates,

increased to 68 percent.[34] Victims "who experienced a direct and indirect financial loss of at least $1 lost an average of $1,769."[35]

That is significant, given that "[n]early [h]alf of America [l]ives [p]aycheck-to-[p]aycheck,"[36] and "49 percent of today's [American] workers have $1,000 or less on hand to pay out-of-pocket expenses."[37] Their "plight is compounded by the fact that the recession ravaged many Americans' credit scores to the point that [most Americans] have subprime credit. That means if emergencies arise, many Americans are forced to resort to high-interest debt from credit

---

anxiety and inconvenience of being denied utility service, time expenditures and psychological stress of dealing with debt collectors, and the distraction of being subject to civil lawsuit or criminal investigation." Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1062, 1094 (2009) [hereinafter, Romanosky & Acquisti, *Privacy Costs*], *citing* Katrina Baum, *Identity Theft, 2004*, *in* BUREAU OF JUSTICE STATISTICS BULLETIN (2006), *available at* http://www.ojp.usdoj.gov/bjs/abstract/it04.htm (link dead; for a version of the article without graphics and many of the tables, refer to http://www.bjs.gov/content/pub/ascii/ it04.txt).

[34] *Supra* note 31 at 6.

[35] *Id.*

[36] Christopher Matthews, *Nearly Half of America Lives Paycheck-to-Paycheck*, TIME.COM (Jan. 30, 2014), http://time.com/2742/nearly-half-of-america-lives-paycheck-to-paycheck/.

[37] *What is voluntary insurance –and why do employees need it?*, AFLAC, http://www.aflac.com/insights/articles/what_is_voluntary_insurance.aspx (last visited May 1, 2015).

cards or payday loans."[38] Given those facts, it seems easy to understand why nearly 40 percent of Americans experiencing cases of identity theft requiring six months or more to resolve have reported suffering through moderate or severe emotional strain as a result.[39] Some have also experienced relationship problems.[40]

Despite all of this, many people seem to struggle with "breach fatigue"[41]—possibly because "the escalating number of data breaches reported in the media may [have facilitated] psychological *habituation*," desensitizing them to data breaches.[42] Still, lawsuits related to data breaches do occur. For this and other reasons, many companies have insurance to deal with such lawsuits.[43] Importantly, some companies have provided, or helped to provide, their employees with identity theft protection services.[44]

---

[38] *Supra* note 36; *see also infra* note 101 (noting finance-related hardships associated with identity theft can be extremely significant).

[39] *Supra* note 31 at 1, 12.

[40] *Id*.

[41] Seth Rosenblatt, *As Security Breach Reports Mount, Experts Fear Alert Fatigue*, CNET (August 22, 2014), http://www.cnet.com/news/as-security-breach-reports-mount-experts-fear-alert-fatigue/.

[42] Romanosky & Acquisti, *Privacy Costs*, s*upra* note 33 at 1096.

[43] Deirdre Fernandes, *More Firms Buying Insurance For Data Breaches*, BOS. GLOBE (Feb. 17, 2014), *available at* http://bit.ly/1jxAdHP.

[44] *E.g., Alcott Offering Employees Identity Protection & Privacy Management Tool*, ALCOTT HR (May 26, 2011), http://www.alcottgroup.com/alcott-offering-employees-identity-protection-privacy-management-tool/1803/ (details protection plan), Richard G. Clarke, *Is ID Theft Insurance Worth Recommending to Agency Clients?*, INS. J. (Oct. 9,

II. POPULAR MEANS OF HELPING EMPLOYEES AFTER DATA BREACHES ARE INADEQUATE

Given the background information about data breaches provided above, it seems data breaches will remain an unfortunate fact of life—barring an apparently elusive change in attitudes, technology, and policies.[45] Unfortunately, the popular means of preventing and mitigating losses to employees whose information has been exposed—i.e., breach notifications, ex post defensive efforts, and lawsuits—are inadequate.[46]

2008), http://bit.ly/1G0yQPC [hereinafter, Clarke, *Worth Recommending*].

[45] There are other reasons for suspecting that this is the case for reasons not mentioned above. These include, but seem unlikely to be limited to, the following. For instance, regulations "that require specific technologies such as data encryption may be misguided. One commentator argued that such efforts would create a security floor that may meet current needs but would soon be insufficient. Moreover, data encryption, while possibly useful at preventing unauthorized access, would not affect the probability of a successful cyber-attack." Romanosky & Acquisti, *Privacy Costs*, s*upra* note 33 at 1091-1092. Furthermore, "[b]y abiding by a series of guidelines or commandments, firms cease to be proactive in protecting against future computer attacks, privacy violations and data breaches." *Id.* at 1092. Nor is the "the cloud" expected by information technology and security professionals to offer salvation from data breaches in the form of industry-standard security that all can cheaply buy into. *See,* Press Release, Netskope, Netskope and Ponemon Institute Report: IT Estimates Increased Use of Cloud Services Can Triple the Probability of a $20M Data Breach (June 4, 2014), http://bit.ly/1cGq8ei.

[46] Romanosky & Acquisti, *Privacy Costs*, s*upra* note 33, at 1101 (Article reviews personal data protection efforts in America using three economic theories: ex ante safety

The most powerful single reason for that conclusion is that those answers are predicated upon the *detection* of data breaches. That reason is examined below, as are others.

A. DATA BREACH NOTIFICATIONS ARE INADEQUATE

Nearly every American state requires businesses which detect a breach in their data systems, to notify all potentially affected parties.[47] This could conceivably benefit employees in two ways. First, affected employees could take measures to protect themselves, or the law could require they be provided with identity protection services. Second, employees could sue their employers. It should be noted, though, that such responses are rarely possible because most data breaches are not detected.[48] As shall be demonstrated in the following, that point, among

---

regulation, ex post liability, and information disclosure. Concludes in final sentence that these "contemporary policy approaches appear ill-equipped to adequately prevent or mitigate consumer loss due to data breaches." *Id.* The policy approaches applied to consumers and employees seem to be essentially the same. E.g., notifications.)

[47] *Global HR Hot Topic—May 2012: Data Breach Notification and the Multinational Employer*, WHITE & CASE (May 2012), http://www.whitecase.com/hrhottopic-0512/#.VOkj_fnF-ZR (includes links to the text of the 48 laws adopted by 48 states as of 2012 pertaining to data breach notification).

[48] *Supra* note 16, 17, 18, 20 and accompanying text. While that criticism is seemingly the simplest and most powerful, there are other criticisms about notifications that could be raised. *E.g.,* notifications only reduce identity theft by 6.1 percent, on average. Sasha Romanosky et al., *Do data breach disclosure laws reduce identity theft?*, 30 J. OF POL'Y ANALYSIS & MGMT. 256, *available at* http://bit.ly/1bIW8wU.

others, point, among others, counts against those responses and breach notification laws.

B. POPULAR EX POST DEFENSIVE EFFORTS ARE INADEQUATE

Besides litigation, there are two popular means of defending against identity theft-related problems that can arise from a data breach: protect one's identity by oneself, or have someone else help do so. In America, laws have been proposed that would require certain entities to provide identity protection services to individuals whose identity information is compromised by the breach of databases maintained by those entities. Those laws could obviously work in tandem with breach notification laws, but few such laws seem to have been implemented, though.[49]

---

[49] Personal Data Protection and Breach Accountability Act of 2014, S.1995, 113th Cong. (2014), *available at* https://www.congress.gov/bill/113th-congress/senate-bill/1995/text [hereafter, S.1995] (example of pending legislation); CAL. CIV. CODE § 1798.82 (West 2015) (example of implemented legislation). The latter legislation, implemented in 2015, "appears to impose the country's first requirement to provide free identity theft protection services to consumers in connection with certain breaches." *See* Nathan D. Taylor & Patrick Bernhardt, *Breaking Old Ground: California Again Amends Breach Law*, MORRISON & FOERSTER LLP 1 (Oct. 9, 2014), *available at* http://www.mofo.com/~/media/Files/ClientAlert/2014/10/141009CaliforniaAgainAmendsBreachLaw.pdf (making statement in reference to California Assembly Bill 1710, which gave rise to amendments to Cal. Civ. Code § 1798.82 implementing the requirement); *see also*, Privacy—Confidential or Privileged Information—Identity Theft, 2014 Cal. Legis. Serv. Ch. 855 (A.B. 1710) (West) (noting amendments made by California's AB-1710 to Cal. Civ. Code § 1798.82 which gave rise to aforementioned requirements).

Regardless of that, in relation to both implemented and proposed laws, the time-limited nature of the required protection usually renders it potentially unsatisfactory.[50] As for the possibility of individuals trying to protect their own identities after a breach, that has been dismissed by numerous authors as enormously impractical or impossible.[51] There are other limitations to these defense efforts. One is that individuals do not always simply embrace the notion of having to guard their compromised identities for the rest of their lives. Given all of these limitations, people sometimes use litigation to seek remedies after a breach.

C. LITIGATION IS INADEQUATE

Lawsuits can be useful for providing redress for harms and changing behavior. However, litigation predicated upon data breaches cannot occur if potential plaintiffs do not know from whom—e.g., Sony—their information was stolen. The fact that the exact source of most data breaches is not known might thus preclude most litigation

---

[50] *E.g.,* CAL. CIV. CODE § 1798.82 (West 2015), *supra* note 49 ("If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months…"); S.1995, *supra* note 49 ("Regardless of the method by which individual notice is provided to individuals under section 213(1), such notice shall include...notice that the individual is entitled to receive, at no cost to such individual...credit monitoring or any other service that enables consumers to detect the misuse of sensitive personally identifiable information for a period of 2 years."). It seems one or even two years of identity protection is inadequate. *Infra* notes 65-68 and accompanying text.

[51] *Infra* notes 100-102 and accompanying text.

over data breaches. This obviously severely limits the utility of litigation.

Yet, even when litigation is not precluded in this way, it is of limited utility—and there are reasons to believe it might remain so.[52] These reasons relate to the incidence of litigation pertaining to data breaches; the claims, causes of action, and parties involved in the litigation, and the ways in which the litigation generally ends.

1. Incidence of Litigation

With respect to the incidence of litigation in connection with data breaches, it should be noted that from 2005 to 2010, 4 percent of publicly reported data breaches resulted in federal litigation.[53] While that information provides only part of the picture, given that "many of the most prominent data security cases to date were filed in state court,"[54] it is a useful and thought-provoking

---

[52] This can be seen by referring to the findings of a groundbreaking study published in 2012, along with other information, as will be done shortly. Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation,* 11 J. OF EMPIRICAL LEGAL STUD. 1 (2014) *available at* http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf. It should be noted that this study focused primarily on litigation heard before federal courts. However, the authors of the study stated that, "under the Class Action Fairness Act (CAFA, 2005), we are relatively confident that all large class actions (and certainly multistate actions) would, indeed, be either filed in, or removed to, federal court. Conversations with defense attorneys strongly support this intuition. Moreover, the absence of these suits would not bias our regression estimates…" *Id.* at 19.

[53] *Id. at* 24.

[54] David A. Zetoony et al., *Data Breaches: Will You Be Sued, And Can You Lower Risk?*, L. 360 (Apr. 25, 2012), *available*

metric.[55]

2. Claims, Causes of Action, Parties

Some data breach lawsuits are brought by public entities (e.g., state attorneys general), but the lawsuits are typically private class actions.[56] The defendants in the cases are often large businesses.[57] Generally, redress is sought for one or more of the following: actual harms from identity theft (e.g., financial fraud), emotional distress, costs of future loss prevention (e.g., identity theft insurance and credit monitoring), and the elevated chance of future harms.[58] The complaints brought can consist of one or more of at least eighty-six causes of action, representing a range of common-law and statutory causes of action.[59]

3. Cace Outcomes

Cases "generally either settle, or are dismissed, either as a matter of law, or because the plaintiff was unable to demonstrate actual harm

---

at http://www.law360.com/articles/333408/data-breaches-will-you-be-sued-and-can-you-lower-risk.

[55] Useful enough for Professor of Law, Daniel Solove, to reach some wide-ranging conclusions about the utility and functionality of litigation. *See supra* note 70.

[56] *Id.*

[57] *Id.* Which suggests that lawsuits are, at least, not the primary reason for which small businesses experiencing data breaches go out of businesses.

[58] *Supra* note 52 at 4.

[59] *Supra* note 52 at 20 ("We found 34 different kinds of tort causes of action, 15 contract, 4 violations of state statutes, and 33 violations of federal statutes.").

caused by the data breach."[60] To date, there have been numerous settlements related to data breaches.[61] The settlements offered are often not geared toward fixing any future damage, and if they are, it is to a limited degree. A review of the details of these settlements, and of pre-litigation offerings, illustrates this point. Settlements sometimes limit the period in which companies can be sued in pursuit of identity theft-related compensation.[62]

---

[60] *Id.* at 4. The details of the basis for these dismissals as matters of law or due to failure to demonstrate actual harm are as follows. Frequently, "there is little or no evidence about what happened to the [information] once it left the defendant's control." Paul Karlsgodt, *Key Issues in Consumer Data Breach Litigation*, PRAC. LAW THE J. 48, 51 (Oct.-Nov. 2014), *available at* http://bit.ly/1PB4Oms. As such, plaintiffs "often cannot plead any actual financial harm or identity theft arising from the loss of data, either because of the lack of evidence or the nature of the information accessed, or because the plaintiffs were reimbursed for any financial loss that occurred within the payment card system. Accordingly, plaintiffs' principal theory of harm is that the loss of [their information] puts them at higher risk of future identity theft. Most federal courts agree that the mere possibility of future harm is not enough to create an injury-in-fact sufficient to confer standing... A minority of courts…have found facts falling short of actual financial loss to…confer standing… Even where standing was found, however, often the court still dismissed the complaint at the pleading stage based on the plaintiffs' failure to allege sufficient injury to establish the elements of their claims." *Id.*

[61] *See*, *Chronology of Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breach-asc (provides information about 4,517 breaches).

[62] *E.g., Frequently Asked Questions*, ANTHEM BLUE CROSS SECURITY SETTLEMENT, https://anthembluecrosssecuritysettlement.com/FAQ.aspx [hereinafter, ANTHEM, *Frequently Asked*] (last visited May 8, 2015) ("If you discover later that your identity has been stolen, you have 90 days after you first find out about the

They normally seem to offer one to two years of identity protection services.[63] Rarely do they seem to offer more.[64] The problem with this approach is that after breaches involving information like Social Security numbers, if no one else steals the identity, criminals can use the information for a very long time -- far beyond two years, and seemingly forever if no one else steals the identity[65]

---

identity theft, or until May 31, 2016, whichever comes first, to file a claim for reimbursement...").

[63] A review of 250 out of 4,517 records relating to data breaches found 47 references to the provision of paid protection services in the aftermath of data breaches. In all of these cases, the protection was provided free of charge for one year. *Supra* note 61 (this source, and those linked to from pages two through five at the bottom of the linked page, were reviewed). *But see, Attorney General Reaches Settlement With Wellpoint in Consumer Data Breach*, INDIANA.GOV (July 5, 2011), http://bit.ly/1nGUJIe (two years); *Frequently Asked Questions*, GILARDI & CO. LLC, http://bit.ly/1JAOro2 (two years) (last visited May 3, 2015).

[64] *2012 Consumer Study on Data Breach Notification*, PONEMON INST. LLC 23 (June 2012), *available at* http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf [hereinafter, PONEMON, *Consumer Study*]. Five-year extensions of such services were available in some cases. *E.g.,* ANTHEM, *Frequently Asked*, *supra* note 62; *Blue Cross of California Website Security Cases*, ROBINSON CALCAGNIE ROBINSON SHAPIRO DAVIS, INC., http://www.rcrsd.com/news/california-blue-cross/ (last visited May 8, 2015).

[65] In an article about a data breach involving Anthem and the loss of information that included social security numbers, it is noted that two years of identity theft repair was being offered by Anthem. To this, it is added that "criminals could continue to use the stolen data long after that." Furthermore, it is noted that according to a policy director for Privacy Rights Clearinghouse (a nonprofit), "[f]raud is a never-ending possibility… Consumers have to live with the devastating breach for the rest of their lives." Margot

As such, the plaintiffs in the aforementioned lawsuit relating to the Sony data breach rejected an offer of one year[66] of identity protection services.[67] The plaintiffs instead want five years of credit card and banking monitoring services, identity theft insurance and credit restoration services. In addition, they are "ask[ing] the court to force Sony to do more to address the potential identity fraud that may follow those affected by the breach indefinitely."[68] That the plaintiffs are asking for five years of identity protection services, while requesting that something be done to help deal with the potentially indefinite threat posed by the breach, is interesting. It is suggestive of litigation's limited ability to provide adequate remedies relating to data breaches.[69]

One may wonder whether these limitations are surmountable. Based upon a review of the study

---

Roosevelt, *Does Anthem's Identity Protection Plan Leave Victims Vulnerable?*, ORANGE COUNTY REG. (March 19, 2015), *available at* http://www.ocregister.com/articles/credit-654714-bureau-monitoring.html; *see also, infra* notes 66-68 and accompanying text.

[66] Ben Fritz & Danny Yadron, *Sony Hack Exposed Personal Data of Hollywood Stars*, WALL ST. J. (Dec. 5, 2014), *available at* http://on.wsj.com/1vF24yt.

[67] Lucy C., *Week Adjourned: 12.19.14 – Sony, Graco, Comcast*, LAWYERSANDSETTLEMENTS.COM (Dec. 19, 2014), http://bit.ly/1E1f2pA ("[T]he lawsuit alleges that federal agencies have acknowledged that hackers sometimes hold stolen data for over 12 months and that identity fraud can continue to be a threat for many years.").

[68] *Id.*

[69] *See, e.g.*, Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255 (2005); Courtney M. Cox, *Risky Standing: Data Breach, Leaks, and Injury-in-Fact*, SOC. SCI. RES. NETWORK (May 31, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341709.

yielding the findings about litigation and data breaches, discussed above, privacy expert Donald J. Solove concluded that they are. According to Solove, "[o]ur current [legal] system is not dealing with data breaches very well. This research study shows that parties are bargaining around the legal system to make it go away. We need to rethink the concept of harm for data breaches, and we also need to rethink the legal system that handles the cases."[70] Yet, it is not clear how any of this rethinking would yield a way for litigation to overcome the fact that most data breaches are not detected.[71]

D. THE COLLECTIVE IMPLICATIONS OF THE INADEQUACIES: A NEW APPROACH IS NEEDED

There are several implications of the inadequacies of the popular approaches discussed above. It appears to be a bad idea to predicate an approach to helping employees post- data breach upon detecting a breach in a company's system, and then proceeding from there. Does not seem to lend itself to dealing with the problem in or near its entirety now or in the near future. While we cannot always detect the source of data breaches, the damage they cause to victims of identity theft can frequently be detected.[72] Similarly, the damage can

---

[70] Daniel J. Solove, *Why Do Lawsuits for Data Breaches Continue Even Though the Law Is Against Plaintiffs?*, TEACH PRIVACY (Sept. 22, 2014), *available at* http://bit.ly/1KVQOTD.

[71] *Supra* note 16, 17, 18, 19, 20 and accompanying text.

[72] *See, Signs of Identity Theft*, FED. TRADE COMM'N (July 2012), http://www.consumer.ftc.gov/articles/0271-signs-identity-theft [hereinafter, FED. TRADE COMM'N, *Signs of Identity Theft*].

almost always be corrected.[73]

Those realities suggest we need a statutory system putting more emphasis on efficiently detecting and remediating damage to employees, rather than on detecting breaches and preventing damage from occurring in the first place. A new approach for serving that purpose might succeed where the law currently fails to protect employees after data breaches.

IV. A NEW MEANS OF HELPING EMPLOYEES AFTER DATA BREACHES: THE IDENTITY PROTECTION MANDATE (IPM)

Given the considerations raised above, I propose the following to protect employees from data breaches whether or not the breaches are detected.

Companies should have to purchase or help purchase identity theft monitoring and insurance services for their employees. Or, to ensure that most of them do, they should be given encouragement to implement the same measures .[74] Employees must pay only a small percentage of the costs, if any. The

---

[73] *Identity Theft Law*, HG.ORG, www.hg.org/identity-theft.html [hereinafter, HG.ORG, *Identity Theft Law*] (last visited May 8, 2015) ("Almost any kind of damage to a victim's credit or reputation can be effectively undone with the help of experienced legal counsel."); *see also*, SOC. SEC. ADMIN., IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER 7-8, http://1.usa.gov/1CLTguX[hereinafter, SOC. SEC. ADMIN., *Identity Theft*] (last visited May 8, 2015) (noting it is possible to reset one's social security number).

[74] To incentivize the voluntary adoption of this approach, or make the forcible application of it more palatable, employer-based sources of such protection should not be taxed, and payment for such sources should be exempt from income taxation.

rates charged to employers for the provision of such protections should vary depending upon the other measures they have taken to prevent data breaches, and their history with respect to data breaches. In exchange for acquiring such coverage, employees must to some degree waive their right to sue in connection with *all* data breaches. In exchange for expanding employer-based identity protection, identity theft protection services must change the way they deal with employees with preexisting identity problems seeking coverage through group plans. They must not deny them coverage based on these preexisting problems, or charge them more for these preexisting problems if there are indications they stem from workplace data breaches. They must guarantee renewability of plans, and offer to provide services to all workgroup applicants. Lastly, the identity protection services provided to employees must meet minimum standards.[75]

This proposal, referred to in the following as the Identity Protection Mandate (IPM), is evaluated below based upon two familiar models: employer-based health insurance and workers' compensation. Before that is done, though, the value of identity theft monitoring and insurance for employees faced with potentially being harmed by identity theft must be established. For if monitoring and insurance have no value as some suggest, they cannot help employees.

---

[75] Others have analyzed what should be sought when purchasing these services. *E.g., Fact Sheet 33: Identity Theft Monitoring Services*, PRIVACY RTS. CLEARINGHOUSE, http://bit.ly/1Ise4dP (last visited May 3, 2015).

A. IDENTITY PROTECTION SERVICES: WHAT THEY PROVIDE, COST AND ARE WORTH

Some have questioned the value of identity theft monitoring and insurance.[76] This section addresses the following: (1) what the services provide, (2) how much they cost, and (3) how valuable they are.

1. What the Services Provide

What many companies offering a single "identity theft protection" service are referring to with this term are a bundle of features including, but often not limited to monitoring, notification and resolution assistance.[77] The features can differ from each other in terms of exactly what they involve. What they *can* involve is explained in the following sections, and often seems possible because "[t]ypically, [subscribers] give these services a limited power of attorney, which allows them to act on [the subscribers'] behalf."[78] It should be noted that there are companies offering single "identity theft protection" services that offer all three

---

[76] Alina Tugend, *Preventing Identity Theft Without Paying Monthly Fees*, N.Y. TIMES (Feb. 10, 2012), *available at* http://nyti.ms/1bIM47a ("Matthew Davis, a victim adviser at the nonprofit Identity Theft Resource Center, said that 'you have to be a proactive consumer, but I would disagree that no products are helpful.'").

[77] *Identity Theft Protection Services Review*, TOP TEN REVIEWS, http://identity-theft-protection-services-review.toptenreviews.com/ [hereinafter, TOP TEN REVIEWS, *Services Review*] (last visited May 3, 2015).

[78] *Identity Theft Protection Services*, FED. TRADE COMM'N (July 2012), http://1.usa.gov/1FYn3Bt.

features, and cover virtually all aspects of what the features can involve. .[79] Those are the best and most expensive services, and are what the IPM seeks to provide to employees.

a. Monitoring for Indications of Identity Theft

Some of the more expensive monitoring services involve monthly[80] retrieving and scouring what can be described as "records" pertaining to the subscriber. They also involve sending the subscriber summaries of the records and possibly copies of the records themselves. The records subjected to this treatment are generated and retained by entities other than the subscriber—e.g., credit bureaus—and indicate what is being done

[79] That is to say, there are services covering every conceivable angle and form of protection. These include, for example, Lifelock's "LifeLock Ultimate Plus" service, and LegalShield's "Identity Theft Premium" service. TOP TEN REVIEWS, *Services Review*, *supra* note 77 (LifeLock service reviewed); *Identity Theft Plans*, LEGALSHIELD, www.legalshield.com/legalshield-plans/identity-theft/identity-theft-plans/ (last visited May 8, 2015) (LegalShield service); *Identity Theft – Ratings Comparison*, MYNAMEHASBEENSTOLEN, http://www.mynamehasbeenstolen.info /#IDTLELP [hereinafter, MYNAMEHASBEENSTOLEN, *Ratings*] (last visited May 8, 2015) (LegalShield reviewed).

[80] *How TrustedID Credit and Identity Theft Protection Works*, TRUSTED ID, https://www.trustedid.com/products.php?idessentials=how_it_works [hereinafter, TRUSTED ID, *Protection Works*] (last visited May 9, 2015); *Defender Identity Theft*, WHITFIELD CNTY. SCHOOLS, http://wcsbenefits.com/index.php/2015-benefits/defender-identity-theft [hereinafter, WHITFIELD CNTY. SCHOOLS, *Defender Identity Theft*] (last visited May 9, 2015).

with the subscriber's identity.[81] Unsurprisingly, the more expensive the service, the greater the variety of records monitored. The records can reflect, among other things, criminal activity (including, but not limited to, sex offender registries); credit reports; information on websites, such as black market websites; bank accounts; loans or leases; and medical insurance.[82]

b. Notification of Detection of Identity Theft

Information yielded by monitoring can allow the subscriber and the service to determine that the subscriber's identity has been stolen. In other words, it allows for notification of identity theft. Upon reviewing the summaries of their activities, subscribers can determine whether they have been the victims of identity theft. This might

---

[81] *What is identity monitoring or "identity theft protection" service?*, CONSUMER FIN. PROT. BUREAU (Sept. 29, 2014), http://1.usa.gov/1zRnWL3 (retrieving and scouring); WHITFIELD CNTY. SCHOOLS, *Defender Identity Theft*, *supra* note 80 (provision of summaries); TRUSTED ID, *Protection Works*, *supra* note 80 (provision of summaries); Kim Komando, *How To Protect Yourself From Identity Theft (For Free)*, FOX NEWS (Nov. 3, 2012), http://fxn.ws/1QzQqgA (provision of copies of records).

[82] TOP TEN REVIEWS, *Services Review*, *supra* note 77; *see also* Identity Theft Shield (Member & Spouse), LEGALSHIELD, http://bit.ly/1EuCewV (last visited May 5, 2015) ("Proactive searches of applicable local and national databases will be made on your behalf to look for information you may not be aware, including: criminal activity in your name in your county's records and certain federal watch lists, Department of Motor Vehicle records in your state, unknown addresses affiliated with your name, and banking activity in your name reported as fraudulent.").

be because the summary sent to the subscriber by the service indicates that the subscriber has leased a Porsche when that is not the case. The subscriber would then alert the service of this. Alternatively, the service provider might independently conclude that the subscriber is a victim of identity theft, or is in danger of becoming one. For example, if a subscriber's name and Social Security number appear on a black market website, the subscriber would be notified that the security of their identity has been compromised.[83]

c. Recovery of Identity

Once the potential for, or occurrence of, identity theft has been detected, and the identity theft protection services and subscriber know of it, the services can assist subscribers. This can be via non-monetary recovery assistance, or monetary recovery assistance involving insurance. For some of the services offering such assistance, though preexisting identity theft problems are grounds for denying the assistance (hence the IPM's treatment of such denials). [84]

---

[83] *E.g., Our Product*, PROTECTMYID, http://www.protectmyid.com/our-product-benefits/ (last visited May 5, 2015) ("We'll alert you via text or email of new activity that could be identity thieves at work."); LIFELOCK, http://www.lifelock.com/ (last visited May 5, 2015) ("When we find something suspicious, we'll let you know through our patented LifeLock Identity Alert system.").

[84] *E.g., ITRC Fact Sheet 132 - Identity Theft Products*, IDENTITY THEFT RES. CTR., http://www.idtheftcenter.org/Fact-Sheets/fs-132.html (last visited May 9, 2015); *ID TheftSmart*, ID THEFTSMART 1, *available at* https://www.udel.edu/it/response/kbroc.pdf; CONSUMER FED'N OF AM., NINE THINGS TO CHECK WHEN SHOPPING FOR IDENTITY THEFT SERVICES 2,

If assistance is provided in the form of non-monetary recovery assistance. this could mean "dedicated identity theft specialist teams, who can help victims through the difficult and often time consuming process of sorting out any fraudulent activity on their credit reports and existing accounts, and regaining control of their identity."[85] Companies offering the most expensive services may offer help as significant as assigning licensed private investigators to help subscribers regain their identities by doing nearly all of the necessary work.[86]

Monetary recovery assistance offered by the services can take the form of insurance. The

---

http://bit.ly/1F0Kqs8 (last visited May 9, 2015); LAFAYETTE POLICE DEP'T, CRIME PREVENTION BULLETIN 2, http://www.lafayette.in.gov/egov/docs/1362082172_782165.pdf.

[85] This might involve helping them contact proper authorities and credit bureaus. TOP TEN REVIEWS, *Services Review*, *supra* note 77.

[86] MYNAMEHASBEENSTOLEN, *Ratings, supra* note 79 ("The investigator assigned to you handles nearly all of the work *on your behalf*. You must still do certain things that a service cannot legally do on your behalf such as filing a police report. This is vastly superior to typical 'resolution' services that only assign a specialist to help you through the process. The investigator works on your behalf with credit card companies, financial institutions, all three credit repositories, Federal Trade Commission, Social Security Administration, DMV, US Postal Service, law enforcement personnel and any other organizations that may be affected. Fraud alert notifications are sent on your behalf to all three credit repositories, SSA, FTC, USPS, and affected credit card companies and financial institutions. Further, proactive searches of applicable local and national databases are made on your behalf to look for information you may not be aware of including criminal activity in your name, DMV records, unknown addresses, and fraudulent banking activity.")

insurance may underwrite expert assistance (e.g., the cost of retaining a lawyer), and financial relief (e.g., coverage of any wages lost while resolving identity theft problems).[87]

2. The Cost of the Services is Reasonable

The cost to employers of providing employees with protection services that offer the best features seems reasonable. The cost of an all-in-one identity theft protection plan is $120-300 annually when purchased as an individual through the individual market, or between $15-50 through employment-based work group markets.[88] There are many providers of such employment-based services, meaning competition drives down pricing and increases value.[89] Admittedly, many policies place restrictions on the amount of money spent to

---

[87] TOP TEN REVIEWS, *Services Review*, *supra* note 77. As for money stolen from bank accounts by identity thieves, this is usually not covered because when "a fraudster drains your bank account…your bank's zero-liability policies should take care of that." Priya Anand, *Is identity-theft insurance a waste of money?*, MARKETWATCH (Mar. 31, 2014), http://www.marketwatch.com/story/is-identity-theft-insurance-a-waste-of-money-2014-03-31.

[88] Adam Levin, *Consumer Reports Got It Dangerously Wrong on Identity Theft*, HUFFINGTON POST (Mar. 19, 2013), www.huffingtonpost.com/adam-levin/consumer-reports-got-it-d_b_2904286.html (indicating costs); TOP TEN REVIEWS, *Services Review*, *supra* note 77 (indicating bundling of services in sampling of companies).

[89] Gil Lowerre & Bonnie Brazzell, *Look, then leap into voluntary*, BENEFITSPRO (Dec. 13, 2013), http://bit.ly/1cShMzz (29 percent benefits brokers, 45 percent voluntary/worksite brokers).

restore an individual's name, and have deductibles ranging from $100 to $500. Careful consideration of potential policies as to that consideration is thus in order—though there are more expensive alternatives.[90] Nonetheless, the simple fact is that employers *can* provide employees access to high quality identity protection services at a maximum yearly cost of about $50 per employee. That seems very affordable, and well worth spending given the value of the services it can buy.

3. The Services Are Valuable

Identity theft monitoring and insurance are valuable for reasons relating to monitoring and insurance.

b. The Value of Insurance

---

[90] Hal Bundrick, *Should You Buy Identity Theft Insurance?*, U.S. NEWS & WORLD REPORT (Mar. 24, 2014), *available at* http://bit.ly/1hUBxDs [hereafter, Bundrick, *Should You Buy*]. Some have suggested a simpler, though more expensive way of dealing with this consideration: the purchase of prepaid legal services without such restrictions. Karen Pallarito, *Employers Offering ID Theft Protection As Voluntary Benefit*, BUS. INS. (Feb. 8, 2009), http://bit.ly/1FIvphY. However, the cost of a prepaid legal service providing coverage of legal aid without the restrictions would increase costs by a minimum of $8-$16 per month, and a maximum of $23-$26 per month per employee. *Id.* Obviously, adopting the prepaid litigation coverage alternative to carefully considering and selecting polices could thus become rather expensive. Choosing to ignore these considerations would be wrong. Coverage of legal fees is important, as "[a]lmost any kind of damage to a victim's credit or reputation can be effectively undone with the help of experienced legal counsel." HG.ORG, *Identity Theft Law*, *supra* note 73.

Simply put, the value of identity theft insurance is that it provides coverage for the cost of reclaiming one's identity, such as taking time off work and hiring an attorney.[91] That is valuable, given that in recent years, "victims [of identity theft] who experienced a direct and indirect financial loss of at least $1 lost an average of $1,769,"[92] nearly "[h]alf of America [l]ives [p]aycheck-to-[p]aycheck,"[93] and "49 percent of…[American] workers have $1,000 or less on hand to pay out-of-pocket expenses."[94] Monitoring services' value is not so simply established.

b. The Value of Monitoring

Monitoring services are valuable for three reasons. First, while most of what they do involves actions that virtually anyone can conceivably carry out themselves for less money, in reality many people would be unable or unwilling to take these actions. Second, monitoring services might allow for data breaches suffered by companies that might otherwise go undetected to *be* detected. Third, thanks to the benefits noted in the two preceding points, monitoring services might facilitate faster detection of data breaches and identity theft.

i. People Are Often Unable or Unwilling to Do What Monitoring

[91] *Supra* note 87 and accompanying text.
[92] *Supra* note 31 at 6.
[93] *Supra* note 36.
[94] *Supra* note 37.

Services Can Do

As stated above, monitoring services are valuable because people may not be able to do for themselves what monitoring services can do. Among many other examples of such things people might do for themselves are retrieving and reviewing credit scores,[95] searching for criminal records,[96] and contacting one's medical insurer.[97] The alleged ability of people to do these things "by [themselves] for less" is debatable.[98]A cyber branch chief of an intelligence agency under the Department of Defense concluded that, "You can certainly do it yourself; however, I believe that it is not worth the effort involved to protect yourself without paying for a service."[99] Other writings and research support this conclusion.[100] According to

---

[95] *Identity Theft & Credit Card Fraud – How to Protect Yourself*, WALL ST. J., http://guides.wsj.com/personal-finance/credit/how-to-protect-yourself-from-identity-theft/ (last updated May 5, 2015).

[96] *Supra* note 82 and accompanying text.

[97] *Supra note* 76.

[98] *Don't Get Taken Guarding Your ID*, CONSUMER REPORTS (January 2013), http://www.consumerreports.org/cro/magazine/2013/01/don-t-get-taken-guarding-your-id/index.htm [hereinafter, CONSUMER REPORTS. *Don't Get Taken*].

[99] Bundrick, *Should You Buy*, *supra* note 90.

[100] Denise Richardson, *Consumers Find Identity Theft Protection Services Reduce the Impact Of Fraud*, GIVE ME BACK MY CREDIT (Mar. 11, 2011), http://bit.ly/1RsTmx5 ("[I]dentity theft protection services…make themselves worth whatever nominal money you pay for them [because t]hey not only help reduce your risk, but…help you recover, and clean up the mess… Time is money, and if you have to spend your time cleaning up after an identity theft, you could lose work hours, which means less money in the bank at the end of the month. These days, that can mean the difference

another commentator, the "often mind-numbing minutia of the proliferating identity theft risk-reduction strategies often exceed the bounds of what might be reasonably expected from most citizens in managing a single risk."[101] Monitoring services thus allow people to have done for them what they cannot do for themselves.

ii. Monitoring Services Might Allow Detection of Otherwise Undetected Data Breaches

Monitoring services could provide another benefit otherwise unobtainable: they could provide

---

between making it and breaking it. Identity theft protection services restore your lost peace of mind and could keep you and your family from falling off the deep end."), *citing, Identity Theft Costs Time and Money; Study Finds That Identity Theft Protection Services Can Help*, GLOBENEWSWIRE (Mar. 8, 2011), http://www.globe newswire.com/newsroom/news.html?d=215695 [hereinafter, GLOBENEWSWIRE, *Time and Money*] (Finding "victims who claimed to have ITPS [identity theft protection service] at the time of identity theft fraud (relative to those with no ITPS at the time of the identity theft fraud): [s]pent significantly less time to resolve issue (average self-reported hours spent: 45 hours vs. 86 hours); [e]xperienced significantly less time till their identity is recovered (average self-reported weeks involved: 5.3 weeks vs. 20.2 weeks)[;] and [h]ad to personally outlay less money (average self-reported dollars spent: $345 vs. $1,109).") *See also supra* note 36, 37, 38 and accompanying text (explaining how financially insecure many Americans are).

[101] Jennifer R. Whitson, *Identity Theft and the Challenges of Caring for Your Virtual Self*, INTERACTIONS 44 (March-April 2009), *available at* http://bit.ly/1RsTrkb.

two means of detecting an otherwise undetectable breach of a company's data. In both instances, the means of detection would be predicated upon two elements: (1) the security of the identity of every employee at a company being monitored by a single identity protection service, and (2) the service knowing the same company employs all of the individuals.

As such, one way to detect that a company has suffered a data breach—which as far as can be determined has not been suggested elsewhere—might depend upon analyzing the incidence of identity theft among those employees. The incidence, in terms of rate or chronology, might allow deductions to be made by the identity protection services and employees: e.g., the employer of the employees has suffered a data breach, or another company with which the employer does business in relation to its employees (e.g., an insurance company) has suffered a data breach. Thus, monitoring services might help expose otherwise undetected data breaches.

Much the same might be accomplished thanks to other activities of monitoring services that most individuals likely cannot not replicate. These activities include scanning black market internet chatrooms and other places for evidence that one's data is being sold by criminals.[102] Far from that being useless because "if crooks are found to have your ID data, you can't get it back from them,"[103] as has rather foolishly been suggested by some, this

---

[102] *What is identity monitoring or "identity theft protection" service?*, CONSUMER FIN. PROT. BUREAU (Sept. 29, 2014), http://1.usa.gov/1zRnWL3 [hereinafter, CONSUMER FIN., *What is Identity*].

[103] CONSUMER REPORTS. *Don't Get Taken*, *supra* note 98.

seems very useful. It might allow one to recognize that a breach of a company's databases has occurred. If information about all of the employees at a business is being sold on a black market website, that might indicate that the business's databases have been breached.[104]

iii. Monitoring Services Can Facilitate Faster Detection of Identity Theft and Data Breaches

The points regarding the value of monitoring that have been discussed suggest another value of monitoring services: that they can facilitate faster detection of data breaches and identity theft.[105] For example, with respect to identity theft, if many people cannot take or are unwilling to take the measures needed to detect identity theft by themselves, they might detect

---

[104] Suppose—for example—the information of half the people working for a company that has purchased, or helped purchase, identity protection for its employees appears at the same time (or roughly so) on black market chatrooms full of criminals trying to buy and sell stolen data. If a monitoring service detected the presence of the employees' information, and knew they were employees of a single company, the service could deduce that their employer might have suffered a data breach and notify the employer.

[105] With respect to identity theft, if many people cannot, or are unwilling to, take the measures needed to detect identity theft by themselves they might detect identity theft more slowly than a monitoring service would. As for data breaches, if data breaches would go undetected without the measures discussed above, then monitoring would facilitate faster detection of data breaches.

identity theft more slowly than a monitoring service would. Such increases in detection speed are important because until their crimes are detected, identity thieves can do what they want with the identities they have stolen. Until the crime is detected, the damage done and the difficulty of fixing it increases. Thus, detecting the problem so that it can be treated sooner rather than later is very valuable.[106]

B. EVALUATING THE IPM USING EMPLOYER-BASED HEALTH INSURANCE AND WORKERS' COMPENSATION

Having established that at the very least, arguments can be made to counter those suggesting that identity theft monitoring and insurance are of little to no value, we now turn to considering WC and EBHI. These systems will be used to evaluate the IPM.

1. Employer-Based Health Insurance (EBHI)

To prepare the EBHI lens for use, background information about the subject will first be provided. This information will cover the history, features of design, and utility of EBHI.

a. Background Information About EBHI

[106] JAVELIN STRATEGY & RESEARCH, 2010 IDENTITY FRAUD SURVEY REPORT: CONSUMER VERSION 14 (2010), http://bit.ly/1bIMOJx; FED. TRADE COMM'N, *Signs of Identity Theft*, *supra* note 72.

i. Paying for Healthcare Prior to EBHI

In 1900, most Americans spent $5 per year on healthcare, primarily because most medical care available was "basically medieval—a bunch of potions that did nothing."[107] People who were poor went to hospitals to die, and the cost of a hospital stay was thus negligible.[108]

This eventually changed. Healthcare and hospital stays not only became lifesaving resources, but also more expensive.[109] This led to hospitals often finding most of their beds empty.[110] As a hospital official at Baylor University Hospital put it, "counter clerk[s] can pay [up to] $1 a month, yet it would take about 20 years to set aside [money for] a large hospital bill."[111]

That same official also noticed that, "We spend a dollar or so at a time for cosmetics and do not notice the high cost."[112] Baylor University Hospital officials consequently sought to get people to pay for hospital visits by having them pay for it in the same way as lipstick.[113]

ii. The Emergence of EBHI

---

[107] Alex Blumberg, *Accidents Of History Created U.S. Health System*, NAT'L PUB. RADIO (Oct. 22, 2009), http://www.npr.org/templates/story/story.php?storyId=114045132.
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*

Baylor University Hospital took a step toward a new approach to payment by offering a deal to a group of school teachers: the teachers would pay 50 cents per month for the hospital to pay all the costs for any of their hospital visits.[114] With the coming of the Great Depression, "almost every hospital in the country saw its patient load disappear," and Baylor's approach thus became somewhat popular.[115] It was available in nearly all states. [116] Yet, few people participated in the system.[117]

With the coming of World War II, though, this changed. Factory owners "needed a way to lure employees," and turned to fringe benefits to do this. They offered increasingly generous health plans.[118]

iii. The Tax Change-Linked Boom in EBHI's Availability

The Internal Revenue Service (IRS) took steps that dramatically increased American participation in EBHI plans.[119] In 1943, the Internal Revenue Service (IRS) decreed that employer-based healthcare should not be taxed.[120] Then, in 1954, the IRS ruled that "health insurance premiums paid by employers were exempt from

---

[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*

income taxation."[121] These actions of the IRS had a tremendous impact upon Americans' participation in health insurance plans—driving it from nine percent of the population in 1940, to 63 percent in 1953, and 70 percent by the 1960s.[122] By 1980 it had grown to 79 percent,[123] and by 1990 to 83.5 percent—although it has increased and fluctuated from 83.5 percent, it has never fallen below that number.[124]

iv. Coverage of Preexisting Conditions Under EBHI and the Health Insurance Portability and Accountability Act

Before 1996, preexisting conditions were grounds for being denied health insurance coverage in the United States. However, the Health Insurance Portability and Accountability Act (HIPAA) of

---

[121] *Employer-Sponsored Health Insurance and Health Reform*, THE NAT'L BUREAU OF ECON. RESEARCH, www.nber.org/bah/2009no2/w14839.html (last visited May 8, 2015).

[122] *Supra* note 107.

[123] Robin A. Cohen et al., *Health Insurance Coverage Trends, 1959–2007: Estimates from the National Health Interview Survey*, 17 NAT'L HEALTH STATISTICS REPORTS 1 (July 1, 2009), *available at* http://1.usa.gov/1H8F7aP.

[124] *Percentage of people with health insurance in the United States from 1990 to 2013*, STATISTA, http://www.statista.com/statistics/200958/percentage-of-americans-with-health-insurance/ (last visited May 5, 2015).

1996 limited the exclusion of coverage for preexisting conditions, and raised the premiums for preexisting conditions in EBHI.[125] Costs rose by less than one percentage point in connection with HIPAA.[126] This seems to have been made possible because it applied to a population in which almost everyone was covered.[127] Later developments—particularly the Affordable Care Act—expanded these protections to all Americans, by requiring all people to carry health insurance (with some

[125] *FAQs About Portability of Health Coverage and HIPAA*, DEP'T OF LABOR, http://www.dol.gov/ebsa/faqs/faq_consumer_hipaa.html (last visited May 5, 2015); Stephen H. Long & M. Susan Marquis, *Part II. Potential Effects of HIPAA: A Review of the Literature*, DEP'T OF HEALTH & HUMAN SERVICES (Oct. 1998), http://aspe.hhs.gov/health/reports/hipabase/pt2.htm.

[126] *Final Regulations for Health Coverage Portability for Group Health Plans and Group Health Insurance Issuers Under HIPAA Titles I & IV*, 69 Fed. Reg. 78742 (2004), *available at* http://1.usa.gov/1KVRA2R ("The Departments also note that the estimated $515 million cost associated with extensions of coverage under HIPAA amounts to a small fraction of one percent of total expenditures by private group health plans.")

[127] Bob Semro, *The Role of the 'Employer Mandate' in the Affordable Care Act*, HUFFINGTON POST (July 12, 2013), http://huff.to/1APTfRy [hereinafter, Semro, *Role of the 'Employer Mandate'*] (prior to implementation of employer mandate provision of Affordable Care Act, approximately 94 percent of companies with 50 to 199 employees and 98 percent of companies with 200 or more employees provided health insurance); 42 U.S.C. § 18091 (2) (requirement for individuals to purchase insurance said to be "essential to creating effective health insurance markets in which improved health insurance products that are guaranteed issue and do not exclude coverage of pre-existing conditions can be sold.")

exceptions),[128] and required that some businesses provide health insurance to their employees or pay a penalty.[129] This incorporated other elements into EBHI in the United States. However, any further discussion of the Affordable Care Act seems irrelevant to this analysis.[130]

v. The Legacy of EBHI

The "system of [EBHI] has long provided coverage to the vast majority of America's workers and their dependents."[131] Employers continue to offer health insurance to their employees, and do so for numerous reasons. According to a survey whose results were published in 2013—before implementation of the employer mandate of the Affordable Care Act—responses to the question why small businesses primarily offered health

---

[128] *The Fee You Pay If You Don't Have Health Coverage*, HEALTHCARE.GOV, https://www.healthcare.gov/fees-exemptions/fee-for-not-being-covered/ (last visited May 5, 2015).

[129] *Questions and Answers on Employer Shared Responsibility Provisions Under the Affordable Care Act*, INTERNAL REVENUE SERV., http://www.irs.gov/Affordable-Care-Act/Employers/Questions-and-Answers-on-Employer-Shared-Responsibility-Provisions-Under-the-Affordable-Care-Act (last updated Feb. 18, 2015).

[130] That is because the Affordable Care Act is the product of a system meant to guarantee as much of the American population in general is insured, rather than just employees. It is carefully designed accordingly. *See* Semro, *Role of the 'Employer Mandate,' supra* note 127.

[131] Mark W. Stanton, *Employer-Sponsored Health Insurance*, 17 RESEARCH IN ACTION 1, *available at* http://archive.ahrq.gov/research/findings/factsheets/costs/empspria/index.html.

insurance to employees yielded the following data: 31 percent did it to recruit talented employees, 44 percent because they felt they had a moral obligation to do so, 8 percent for the tax benefits, 8 percent for workplace productivity, and 9 percent for other reasons.[132]

b. Using EBHI to Evaluate the IPM

In considering the Identity Theft Protection Mandate alongside EBHI, several important considerations are raised. These include the following: the relation of the harms to be addressed by identity protection services to any workplace data breaches; reasons employers should offer the services; the degree to which employers have voluntarily offered the services and how that degree could be expanded; and the implications of the expanded services and of potential failures to expand with respect to preexisting conditions.

i. Possible Lack of Connection Between Employment and Problems Covered By the IPM and EBHI Is Surmountable

If identity-related harms can be connected to a workplace data breach, the reasoning behind suggesting that employer-provided identity

[132] *Small Employer Health Insurance Survey*, eHEALTH 5 (Mar. 2013), http://bit.ly/1RsTIUb .

protection should cover them is readily apparent. The reasoning might not be readily apparent if the harms cannot be connected to a workplace data breach. As such, the fact that use of EBHI benefits need not relate to work is important in this context.[133] Like EBHI, there are reasons for which employers might conceivably be unconcerned about whether the identity theft protection they provide is used only in connection to workplace data breaches.

After all, employers already seem to feel compelled to provide identity protection to their employees for the same reason they provide health care, without concern about work connections.[134] Analysis of the reasons for which employers offered health insurance prior to the Affordable Care Act illustrate why that may be the case. As noted above, a survey found that 31 percent of small businesses provide health insurance to recruit talented employees, and 44 percent did it because they felt they had a moral obligation to do so.

ii. There Are Recruitment-Related Reasons for Employers to Embrace EBHI and the IPM

There are reasons to believe that an employer may provide identity protection to recruit talented employees, thereby justifying employer-based identity theft protection for non-work-related problems. Generally-speaking, people with identity

[133] E.g., health insurance would cover treatment of a flu of unknown origin that sickens an employee.

[134] *See, supra* note 147 and accompanying text.

theft protection have "high rates of satisfaction" with the protection and feel they are well served by it.[135] It seems people who do not have such protection might not because it is too expensive for them not because they do not find it desirable.[136] Yet, few employers have noticed this.[137] Evidence suggests many employees would appreciate employer-based identity protection,[138] in the same way they appreciate health insurance. It thus appears identity protection can be used to recruit talented employees.

iii. There Are Morality-Related Reasons for Employers to Embrace EBHI and the IPM

---

[135] *Identity Theft Costs Time And Money; Study Finds That Identity Theft Protection Services Can Help*, THE STREET (Mar. 8, 2011), http://www.thestreet.com/story/11034851/1/identity-theft-costs-time-and-money-study-finds-that-identity-theft-protection-services-can-help.html.

[136] *See supra* note 36, 37, 38 (Americans struggling financially), 88 (cost of protection when purchased via individual market) and accompanying text.

[137] *Infra* note 147 (25 percent of large employers offered identity theft protection coverage to their employees in 2013).

[138] *See,* e.g., Sammer, *Identity Theft*, *supra* note 29 ("Recognizing the growing problem of identity theft, …Wells Real Estate Funds in Norcross, Ga., began offering company□paid identity theft insurance coverage to its employees… The identity theft coverage…is cost-effective relative to the employee relations benefits the company gains… 'It comes with minimal cost, and we get great feedback from employees,' says May."); *infra* note 151 and accompanying text.

Just as there are parallels between recruitment-based reasons for employers to offer health insurance and identity protection, there are also parallel morality-based reasons.

Most small businesses provide health insurance on moral grounds, as noted above, and it seems they might do so because otherwise their employees could not afford it. Employees might struggle to afford identity protection as well. Regardless of those considerations, employees deserve identity theft protection, or assistance to purchase it. Businesses essentially *must* store employee data, which may be subject to breaches,[139] but cannot yet guarantee that the security of that data will not be compromised by a breach[140] or that they will detect a breach.[141] Employees must hand over their data,[142] take the risk that the breach leaking their data will not be detected,[143] and can ultimately be forced to pay to defend themselves if the breach is not detected.[144] If it seems morally right for employers to shield employees via health insurance from health costs for which the employer may *not* be responsible,[145] it arguably makes sense for them to help shield employees from identity theft costs for which the employer may *be* responsible.

It is true employers do not deserve all the blame for data breaches—at least not in all cases—

---

[139] *See supra* note 7.
[140] *See supra* note 24 and accompanying text.
[141] *Supra* note 16, 17, 18, 19, 20, 21 and accompanying text.
[142] *See supra* note 7.
[143] *See supra* note 16,17, 18, 19, 20 and accompanying text.
[144] That is because if the breach cannot be traced to the company or anyone else, the employee will have to shoulder any associated costs by themselves.
[145] *E.g.*, the flu.

given that if they did not keep employee data they could not employ the employees.[146] That is merely a reason to split identity protection costs, rather than force the employee to bear all of them. That would be the ideal way to handle the matter, but while employers have offered identity protection to their employees that has not happened in most cases. The protection is usually offered as a voluntary benefit, and therein lies the problem, as shall be explained in the following

iv. Tax Incentives Might Be Used to Increase Employers' Provision of Coverage Via the IPM, As With EBHI

Despite these important parallels between reasons for offering health insurance and identity protection coverage, employees' access to identity protection via their employers remains limited. That is a parallel with the offering of health insurance early in World War II. In addition, while the numbers of American employers voluntarily offering identity protection has increased significantly over the years,[147] the problem is that in

---

[146] *Supra* note 7.

[147] In 2006, around the same time American employers began offering identity theft protection as a voluntary benefit to employees, only two percent of American employers were making such an offer. M.P. McQueen, *Employers Offer Help Fighting ID Theft*, WALL ST. J. (May 24, 2006), *available at* http://www.wsj.com/articles/SB11484 345472246 1400. By 2013, 25 percent of American employers offered identity

most cases, the protection is offered as a voluntary benefit.[148] Voluntary benefits are "offered through an employer but paid for partially or solely by workers through payroll deferral."[149] By 2013, there were indications that only three percent of employees *had* identity theft protection through their workplace,[150] even though 39 percent of employees allegedly wanted identity theft protection.[151]

In terms of outcome, it seems the current situation relating to employer-based identity theft protection mirrors that of EBHI's early years:[152] employers are not *really* providing it, and it seems the number of them that do will remain unchanged, barring an incentive to do otherwise.[153] Perhaps,

---

theft protection, and 20 percent were planning to offer it. *Voluntary Benefits and Services Survey*, TOWERS WATSON 5 (25 percent), 6 (20 percent) (July 2013), http://bit.ly/1PcoFO2.

[148] Employers offering identity protection as anything other than a voluntary benefit seems to be a rare occurrence. A reason for which this might be the case is that, "[t]he days of employer-paid benefits are disappearing faster than a snow cone in July." Mark Roberts, *5 Benefits of Voluntary Benefits*, BENEFITSPRO (May 28, 2014), http://www.benefitspro.com/2014/05/28/5-benefits-of-voluntary-benefits.

[149] Joanne Sammer, *Getting Results from Voluntary Benefits*, SOC'Y FOR HUM. RESOURCE MGMT (Aug. 9, 2013), http://www.shrm.org/hrdisciplines/benefits/articles/pages/voluntary-benefits-results.aspx.

[150] Carol Patton, *Helping Them Through*, HUMAN RES. EXEC. ONLINE (June 9, 2014), *available at* http://bit.ly/1FeyExz.

[151] LIFELOCK, THE NECESSARY, VOLUNTARY BENEFIT 2, *available at* http://bit.ly/1Ivaf5Z.

[152] *See supra* note 117, 118, and 119 and accompanying text.

[153] There are other metrics by which to arrive at this conclusion. An article in 2008 stated, "Employees are increasingly calling

then, tax reforms might make a difference as they made a difference with EBHI.[154] Allowing the maximum cost of $50 per employee to be written off or even deducted might entice businesses to cover the cost of the coverage. That would allow businesses to offer something to please their existing employees and entice others, while limiting their liability in a fair way.

v. Negative Implications of Failure to Expand Identity Theft Protection Coverage for People with "Preexisting Identity Conditions"

While tax reforms might be a way to expand voluntary offering of identity theft protection, there are consequences if the lack of voluntary offerings

---

for help in the areas of identity theft protection and legal protection." Amanda Buchanan, *Identity Theft Protection Improves Employee Benefits*, BENEFITSPRO (June 25, 2008), http://www.benefitspro. com/2008 /06/25/identity-theft-protection-improves-employee-benefits. In 2008, an article stated that, "Overall, about 3 percent of employers nationwide provided ID theft insurance, according to a 2006 survey by Aon Consulting. The number is expected to rise." Clarke, *Worth Recommending*, *supra* note 44. But by 2011, less than three percent of employers were offering it. John Scorza, *Growth In Voluntary Benefits Expected In 2014*, SOC'Y FOR HUM. RESOURCE MGMT, http://blog.shrm.org/trends/growth-in-voluntary-benefits-expected-in-2014.

[154] *Supra* note 119-124.

persists. As things stand, employees bear the burden of identity theft that may be associated with workplace data breaches, and most employees have not subscribed to an identity theft protection service. This is problematic because if more employees do not ultimately get identity protection, the IPM's coverage requirement as to preexisting identity conditions might not be possible. To understand why that is, it is useful to examine HIPAA.

HIPAA limited the exclusion of coverage and the raising of premiums for preexisting conditions in the context of EBHI.[155] This was partly possible in the United States before the Affordable Care Act because it applied in the employment context, where people having health insurance was the rule, rather than the exception.

There are similarities and differences between HIPAA and the IPM. To examine these, three points must be established. First, many Americans can be said to have a "preexisting identity condition" (PIC) with respect to identity theft and data breaches: approximately 70,156,262 (~22 percent) or 105,234,393 (~33 percent) of 318,892,103 Americans have had their identities stolen if one defines identity theft narrowly or broadly, respectively.[156] Second, that means there is

---

[155] BETH C. FUCHS ET AL., CONG. RESEARCH SERV., THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996: GUIDANCE ON FREQUENTLY ASKED QUESTIONS 4 (1998), *available at* http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/96-805_EPW.pdf.

[156] *See, One-Third of Americans Have Had Their Identity Stolen*, PR NEWSWIRE (Oct. 22, 2014), http://prn.to/1Kz5lUr; CONSUMER FED'N OF AM., TO CATCH A THIEF: ARE IDENTITY THEFT SERVICES WORTH THE COST? 10 (some argue 'identity

a meaningful identity protection gap. So one may conclude that: (1) far less than a quarter of Americans subscribe to an identity theft protection service, and the *vast* majority seem to (2) be very satisfied with the services, and (3) *knowingly* obtain the services independently—not through their employers or companies that have suffered breaches.[157] Third, many identity protection

---

theft' should refer only to someone creating new account with stolen information) and 12 ("22 percent… suffered from new accounts being opened or other frauds being committed using their personal information. That included five percent who said that an identity thief had given their names to the police when stopped or charged with a crime."), (Mar. 2009), http://bit.ly/1Ism1iV *citing* SYNOVATE, FED. TRADE COMM'N, 2006 IDENTITY THEFT SURVEY REPORT 13, 21 (2007), *available at* http://www.ftc.gov/os/2007/11 /SynovateFinalReportIDTheft2006.pdf; *United States*, CIA , https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (last updated Apr. 24, 2015) (population of the United States in December 2014 estimated to be 318,892,103 in July 2014).

[157] In 2013, three percent of Americans had gotten identity theft protection through their employers. *Supra* note 150. The number of Americans who have subscribed to an identity protection service is unclear. In 2011 and 2012, it seems to have been something less than one-fifth of Americans, but a solid majority of them seemed to be pleased with the protection. *See,* William E. Lewis Jr., *Opinion: Identity Theft Protection Services Are A Waste of Money*, KSL (Nov. 21, 2012), http://www.ksl.com/?sid=23029109&nid [hereinafter, Lewis, *Waste of Money*] (indicates that 48 million Americans—i.e., 15 percent of Americans—purchased identity theft protection in 2011); *Most Americans Vulnerable To Hacking, Identity Theft*, ROBERT MORRIS U. 14 (Sept. 11, 2014), http://bit.ly/1F82RfC [hereinafter, ROBERT MORRIS U., *Americans Vulnerable*] (fewer than one-fifth (19.5 percent) of respondents in a poll of 1,001 Americans had identity theft insurance, but 43.1 percent said they were very satisfied with the services, while 47.7 percent were somewhat satisfied, 6.1 percent were somewhat dissatisfied or not at all

satisfied, and one percent were unsure of how they felt); *Investcorp Technology Partners acquires equity stake in leading identity theft protection firm CSIdentity*, INVESTCORP (Jan. 14, 2010), www.investcorp.com/news-and-media/article/investcorp-technology-partners-acquires-equity-stake-in-leading-identity-th ("Approximately 34 million subscribers in the U.S. currently use some form of credit monitoring or advanced identity theft protection services and this is expected to increase over the next few years."); PONEMON, *Consumer Study*, *supra* note 64 at 24-25 (23 percent accepted an offer of identity theft protection in the aftermath of a breach, 89 percent satisfied with identity theft protection services, though 59 percent were not offered identity theft protection services after being notified of a breach); *The Aftermath of a Mega Data Breach: Consumer Sentiment*, PONEMON INST. LLC (Apr. 2014), *available at* http://bit.ly/1J3TZJJ only 25 percent of breach notifications were accompanied by offers of identity theft protection). At the very least, the number of Americans who have purchased the services appear to be holding stable over a period of years—and may even have increased. *Compare* Lewis, *Waste of Money*, *supra* note 157 and ROBERT MORRIS U., *Americans Vulnerable*, *supra* note 157 at 14. (The increase cannot be stated with certainty because the data referenced consists of polls, and the increase is so slight that it might be within margins of error, or driven by recent data breaches yielding the provision of limited-time identity protections services). The identity protection systems (they are systems because while they are similar, they are not the same) offered by at least some of the services thus seem to be working. The services not only provide that which most people can do for themselves but also that which they cannot, and there are indications these services include restoration assistance. *See* Lewis, *Waste of Money*, *supra* note 157 (suggesting that Americans are "purchas[ing] a service to protect [their] good name[s] and reputation[s]," stating that [m]ost of these services are a waste of money as almost all of the services provided are available at little or no cost to the consumer," and referencing monitoring); *see also*, *Does My Homeowner's Insurance Policy Protect Me in the Case Of Identity Theft?*, HOMESITE (Mar. 5, 2009), http://bit.ly/1AQ0s4d ("Identity theft...[v]ictims should have

services do not sell their services to those with PICs.[158]

To ensure that millions of employees with PICs do not fall into a coverage gap, the IPM requires that identity theft protection services change the way they deal with employees with PICs seeking coverage through group plans. Specifically, it requires that they must not charge them more or deny coverage based on these preexisting problems, and must guarantee plan renewability.

For this arrangement to be financially sound, though, most employees might (1) have to subscribe to an identity protection service and (2) not have PICs.[159] That is part of the reason for which the IPM seeks to make having identity protection coverage the norm among employees. As for how many employees have PICs—that is not entirely clear. However, it seems more than a few do,[160] or at least that increasing numbers of them

---

some way of recovering their financial losses...but this…theft is not covered by a basic homeowners insurance policy. Identity theft coverage is available in most states as an optional endorsement on a homeowner's insurance policy...").

[158] *See supra* note 84 and accompanying text.

[159] NAT'L OF INS. COMMISSIONERS, ADVERSE SELECTION ISSUES AND HEALTH INSURANCE EXCHANGES UNDER THE AFFORDABLE CARE ACT 6 (2011), *available at* http://www.naic.org/store/free/ASE-OP.pdf.

[160] In March 2015, the number of part-time and full-time employees in the United States of America was 6.7 million and 119.98 million, respectively. BUREAU OF LABOR STATISTICS, U.S. DEP'T OF LABOR, THE EMPLOYMENT SITUATION—MARCH 2015, at 2 (2015), *available at* http://1.usa.gov/1gck641 (6.7 million); *Monthly Number of Full-Time Employees in the United States From March 2014 to March 2015 (In Millions, Unadjusted)*, STATISTA, http://bit.ly/17cW8mX (last visited May 5, 2015) (119.98 million). Additionally, 70,156,262 or 105,234,393 Americans have been victims of identity theft—depending on how one

will.[161] It would be desirable to make it easy for those with PICs to acquire identity protection while not upsetting the affordability that it seems can and must be achieved in doing so.[162] HIPAA suggests that this can be done with minimal increases in premium and service prices.[163]

Once again, though, that is provided that most employees receive employer-based identity protection coverage. Employers seem to be failing to make sure that most employees receive employer based identity coverage.[164] If that is unchangeable, via tax incentives for instance, then the IPM may have to entice *and* force employers into accepting that they have to make sure their employees have subscribed to an identity protection service. Something along the lines of workers' compensation may thus be necessary. Workers' compensation may be necessary for other reasons as well.

1. Workers' Compensation (WC)

Background information about WC is presented below It covers the history, features of design, and utility of WC. That information is ultimately used to evaluate the IPM.

a. Background Information About WC

---

defines that term—out of a total population of 318,892,103 Americans. *See supra* note 156 and accompanying text.

[161] *Supra* note 15, 16, 17, and 26 and accompanying text.

[162] *Supra* note 88 ($15-$50 through employment-based work group markets).

[163] *Supra* note 126 and accompanying text.

[164] *Supra* note 150.

i. Injury Remedies Before WC

In the early twentieth century, the incidence of workplace injuries spiked in the United States as the number of industrial jobs did.[165] The only legal remedy for injured and disabled workers to pay for medical treatment, and recover lost wages and future income, was to "bring a tort suit against the employer and prove that the employer's negligence caused the injury."[166] This was problematic as employers could and often did use three defenses to defeat employees in the ensuing lawsuits: assumption of risk;[167] the fellow worker defense;[168] and contributory negligence.[169] Consequently, employees rarely prevailed, and faced delays and high costs when they did.[170] Being unable to work and earn money, in addition to legal fees, could thus be ruinous.[171] When employees did prevail, though, employers risked "substantial and unpredictable

---

[165] Jacob Silverman, *How Workers Compensation Works*, HOW STUFF WORKS, http://bit.ly/1Ivb3ru (last visited May 9, 2015).

[166] Ishita Sengupta et al., *Workers' Compensation: Benefits, Coverage, and Costs, 2004*, NAT'L ACAD. OF SOC. INS. 6 (July 2006), *available at* http://www.nasi.org/usr_doc/NASI_Workers_Comp_2004.pdf.

[167] *Id* ("showing that the injury resulted from an ordinary hazard of employment").

[168] *Id* ("showing that the injury was due to a fellow-worker's negligence").

[169] *Id* ("showing that, regardless of any fault of the employer, the worker's own negligence contributed to the accident").

[170] *Id;* GOETSCH, OCCUPATIONALSAFETY, *supra* note 173 at 140.

[171] *Supra* note 165; GOETSCH, OCCUPATIONALSAFETY, *infra* note 173 at 140.

losses."[172]

ii. The Emergence of WC

The costs and inequities of that arrangement created public dissatisfaction and strain in employers' relationships with employees.[173] This led to gradual changes that came to embody WC in the United States. WC "developed as a way to allow injured employees to be compensated appropriately without…[taking] their employer to court."[174]

At the core of WC's ability to do this is the "exclusive remedy doctrine."[175] Under this doctrine, workers to whom WC applies "receive predictable compensation without delay, irrespective of who was at fault [for the injury]."[176] The compensation covers replacement of income and rehabilitation.[177]

---

[172] *Supra* note 166.

[173] Brent Schondelmeyer & Edmund Zalinski, INSURANCE, DICTIONARY OF AMERICAN HISTORY (2003), http://www.encyclopedia.com/topic/insurance.aspx#1 (public dissatisfaction); DAVID L. GOETSCH, OCCUPATIONAL SAFETY AND HEALTH FOR TECHNOLOGISTS, ENGINEERS, AND MANAGERS 142 (Pearson Higher Ed 2011), *available at* http://bit.ly/1Iv4pBG (strain) [hereinafter, GOETSCH, OCCUPATIONALSAFETY].

[174] GOETSCH, OCCUPATIONALSAFETY, *supra* note 173 at 137.

[175] Thomas A. Robinson, *The Future of Exclusive Remedy: Does the Doctrine Still Protect Employers?*, LEXISNEXIS (August 31, 2012), http://bit.ly/1K0j5KZ ("[T]he employee and his or her dependents, in exchange for somewhat modest but relatively assured disability and medical benefits, give up their common-law right to sue the employer for damages for any injury covered by the relevant Workers' Compensation Act.").

[176] *Id.*

[177] GOETSCH, OCCUPATIONALSAFETY, *supra* note 173 at 138.

In exchange for receiving this compensation, employees accept a limited right to sue employers for an occupational injury or disease arising out of or occurring in the course of employment.[178] However, if the worker is unhappy with their compensation package, the worker can appeal to the WC board.[179]

One thing employees need often not be unhappy about is the prospect of their coverage disappearing if the business ceases to exist. Most employers must pay into WC systems, and are required to do so even if they go out of business. Many pay for WC insurance, and the associated rates paid for the insurance depend on a number of factors, including: number of employees, types of work performed (risk involved), accident experience of the employer, potential future losses, overhead and profits of the employer, quality of the employer's safety program, and estimates by actuaries.[180] As such, rates paid by the employers increase as the chance of injury to their employees increases.[181] The principle underlying this is "cost allocation." This is "the process of spreading the cost of WC across an industry so that no individual

[178] *Id.* at 137.
[179] *Id.* at 145.
[180] *Id.* at 144.
[181] Harold Averkamp, *Payroll Accounting (Explanation)*, ACCT. COACH, http://www.accountingcoach.com/payroll-accounting/explanation/4 (last visited May 4, 2015) ("For example, statistics show that a production worker in a meat packing plant has a greater-than-average chance of suffering job-related cuts or back injuries. Because of this, worker compensation insurance rates for these employees can be as high as 15 percent of wages. On the other hand, the office staff of the meat packing plant—provided that they do not venture out into the production area—may have a rate that is less than one percent of salaries and wages.").

company is overly burdened,"[182] by "spread[ing] the cost of WC appropriately and proportionately among industries ranging from the most to the least hazardous."[183]

iii. The Mixed Legacy of WC

What gave rise to WC systems, and the key features of those systems, has now been explained. While these suggest that WC should have a positive legacy, the legacy of WC is difficult to discern. According to some, it is a failure that has not eliminated great expenses or litigation, due primarily to fraud of various kinds that drives up costs and leads to litigation, and medical costs linked with technology.[184] To others, it is a success, though one with imperfections: workers must be paid more for their time out of work, and employers must take control of what happens if an injury occurs to streamline the functioning of the system and to allow employees to return to work quickly.[185] Some have not called for WC to be abolished despite the shortcomings they see in it,[186] while others have suggested it would be wise to do so.[187]

---

[182] GOETSCH, OCCUPATIONALSAFETY, *supra* note 173 at 155.
[183] *Id. at* 138.
[184] GOETSCH, OCCUPATIONALSAFETY, *supra* note 173 at 137-138 (litigation), 156-157 (fraud), 143 (medical technology).
[185] *10 Myths and Facts About Workers' Compensation*, LEXISNEXIS (Dec. 29, 2011), http://bit.ly/1q3tW7U.
[186] *Id.*
[187] Joseph LaDou, *The European Influence on Workers' Compensation Reform in the United States*, 10 ENVTL. HEALTH 103 (2011), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3267658/.

b. Using WC to Evaluate the IPM

The background information about WC that is necessary for evaluating the IPM in relation to WC has now been provided. In considering the IPM in relation to WC for this purpose, the areas of discussion that arise include the following: (1) employers facilitating much of the harm at issue; (2) the abandonment, or near abandonment, of litigation and improved employee access to remedies; (3) service cost differences based upon experience; and (4) potentially skyrocketing costs due to abuses and technological developments. The first four factors can be categorized as being potentially good parallels, and the latter two as potentially bad ones.

i. Many Reasons for Adopting WC Apply to the IPM

i.1 In Each Case, Employers Often Cause Harm to Employees Via Negligence

The degree to which employer negligence facilitates employee harm related to WC and the IPM is one basis for adopting those policies.

Presently, "[m]ost workplace injuries and fatalities are caused by a lack of appropriate equipment and training. Employers are legally obliged to provide both." [188] This seems to be an argument for WC. If employers will not protect the employees from the injuries despite being legally obliged to do so, perhaps they should be legally obligated to help employees deal with the costs of the resulting injuries. Similarly, most data breaches are arguably attributable to employers failing to take preventative measures, despite facing legal consequences for failing to do so.[189] This seems to be an argument for pushing or forcing employers to help employees deal with the costs of breaches, and for implementing the IPM. Of course, one might wonder why litigation could not be used to the same ends.

i.2 In Each Case, Litigation Proved An Ineffective and Expensive Remedy

As noted above, an important basis for the development of WC systems was the shortcomings of litigation as a source of remedies for workplace injuries. Very similar shortcomings are evident as to employees and workplace data breaches.

---

[188] Richard Saint, *Best Foot Forward*, HEALTH & SAFETY INT'L (Sept. 22, 2014), http://www.hsimagazine.com/article.php?article_id=1087.

[189] *Supra* note 23 and accompanying text.

Recall that in the context of WC, employers had defenses that were difficult, if not impossible, to overcome—and that employees' suits therefore often failed. Regarding data breaches, employers also have a defense that is difficult, if not impossible, to overcome: raising the matter of whether there is proof of an actual harm stemming from the breach.[190] If employees win, though, the costs employers face can also vary greatly.[191] That is much like WC. In the context of WC, sometimes employees won and the resulting costs to employers could vary tremendously.[192] There are two other similarities, though they lie in the implications of two key differences between data breach litigation and long-ago litigation relating to workplace injuries.

First, lawsuits are probably often not brought in connection with a breach of an employers' data because the employees and/or employer will never know of the breach.[193] Employees are thus left to shoulder the costs of the harm alone, just as injured employees usually were prior to the emergence of WC in America.[194] Second, litigation over data breaches usually leads

---

[190] *See supra* note 60 and accompanying text.

[191] For instance, according to one study, when suits related to breaches leading to the compromise of individuals' personal information has been brought or threatened but ultimately settled, attorney fees have been a minimum of $8,000, a maximum of $6.5 million, and a mean of $1.2 million. When such suits are settled, the mean value of settlements awarded to each plaintiff has been around $2,500, with a minimum of $500 and a maximum of $15,000. *Supra* note 52 at 20.

[192] *Supra* note 165.

[193] *See supra* 16, 17, 18, 19, 20 and accompanying text.

[194] *See supra* note 165.

to dismissal or inadequate settlements.[195] There is reason to believe it *cannot* lead to anything better.[196] This suggests data breach litigation is arguably, functionally-speaking, as useful to American employees as occupational injury litigation was prior to WC.[197]

These two observations suggest that the key to better protecting employees in the aftermath of workplace data breaches is to do the equivalent of what was done to bring about WC in the United States. That is this: err on the side of looking beyond matters that require the establishment of fault.[198]Look past the detection, notification, and litigation chain to a detection, notification, and resolution chain. Doing that lends itself to serious consideration of something like the IPM, under which employees to some degree waive their right to sue in connection with data breaches , and gain readily available protection from breaches in return.

Employers and employees might experience gains from this arrangement, that they gained, or were supposed to gain, from WC. One example of these gains is that the costs associated with resolving the problems at issue might be reduced by limiting the involvement of lawyers. That would reduce problematic costs linked to litigation over data breaches—costs of a kind that were also problematic with respect to workplace injuries

---

[195] *Supra* note 61-69 and accompanying text.

[196] *See supra* note 8 (most businesses are small), 10 (small business owners struggle to defend against data breaches), 16-20 (many breaches go undetected, and this has been true for nearly two decades) and accompanying text.

[197] *See supra* note 170 and accompanying text.

[198] *Supra* note 176 and accompanying text.

before WC.[199] By avoiding lawsuits over data breaches, employers would remove a potential source of degraded public relations and tension in their relations with employees.[200] That would be similar to how prior to WC, litigation was a source of degradation of such relationships.[201] Last, but certainly not least, employees would gain adequate protection from their employers in the aftermath of workplace data breaches that they typically do not receive via litigation. This would be similar to WC because WC gave employees access to employer-provided remedies they often could not obtain via litigation. With respect to data breaches, such remedies might include the coverage of wages lost trying to resolve identity theft-related issues via insurance gained through the IPM. That would be like WC, which allowed employees to acquire compensation for wages lost while recovering from injuries.[202]

---

[199] *Supra* notes 170-171 (workplace injury litigation costs), 191 (data breach litigation costs) and accompanying text.

[200] *See*, Jon White, *Do Brands Think Data Breaches Have Lost Their 'PR Disaster' Factor?*, PR WEEK (Apr. 14, 2015), www.prweek.com/article/1342479/brands-think-data-breaches-lost-pr-disaster-factor (concluding breaches cause "reputational damage…[that] will impact the ability to gain security-conscious new users"); Donald Harris, *Data Breach Laws A Wake-up Call for HR*, WORKFORCE (Feb. 10, 2006), www.workforce.com/articles/data-breach-laws-a-wake-up-call-for-hr ("[B]reaches involving…employee data will very quickly become an immediate and pressing HR issue by throwing into question the trust in management that is an essential part of good employee relations.")

[201] *Supra* note 166; GOETSCH, OCCUPATIONALSAFETY, *supra* note 173 at 137.

[202] It would also bear strong similarities to the Family and Medical Leave Act (FMLA). The FMLA, "entitles eligible employees of covered employers to take unpaid, job-protected leave for specified family and medical reasons."

These gains might compel employers and employees to support the IPM. Facilitating the existence of these gains may well be a non-negotiable requirement for employers to embrace the IPM, though. That is because the IPM's limitation of the employee's ability to sue their employers might be a non-negotiable condition of employer support for the IPM.

There are several reasons for that. First, it seems the IPM could conceivably increase the possibility that employees, and not only identity protection services, detect a workplace data breach because of the identity protection provided.[203] This could give rise to *more* lawsuits, made possible by

---

Family and Medical Leave Act, DEP'T OF LABOR, http://www.dol.gov/whd/fmla/ (last visited May 6, 2015). These include "tak[ing] care of a seriously ill family member." Linda Meric, *FMLA Anniversary: Celebrating 20 Years of Strengthening Families*, HUFFINGTON POST (February 4, 2013), http://www.huffingtonpost.com/linda-meric/fmla-anniversary-celebrat_b_2615601.html. The FMLA was adopted because society determined it is important for people to be able to balance work and family life by being able to take care of their families, among other things. *Id*; GERALD MAYER, CONG. RESEARCH SERV., R42758, THE FAMILY AND MEDICAL LEAVE ACT (FMLA): AN OVERVIEW 2 (2012), *available at* https://www.fas.org/sgp/crs/misc/ R42758.pdf. Addressing identity theft is arguably another example of that: caring for family by ensuring that one's finances are not harmed. Furthermore, like caring for one's family, it might require time off work occasionally to deal with disasters, or potential disasters. Providing insurance would help families deal with unpredictable losses associated with identity theft, while also protecting employees' paychecks from diminution if employees have to take time off work to resolve identity theft-related issues.

[203] Part IV.A.iii.b.2 ("Monitoring Services Might Allow Detection of Data Breaches Otherwise Going Undetected").

the employer trying to protect the employee.[204] For instance, it might open the door to lawsuits brought by employees via the Private Attorney General Act.[205] Consequently, businesses could face penalties they otherwise would not face.

Employers would probably be unwilling to pay to facilitate such developments. That is why for employers to embrace the IPM, the limitation of employees' right to sue them over data breaches might be necessary. As for people not employed by an employer whose databases may have been compromised, thus exposing the people's information, it would seem unfair to limit their ability to sue. Some could fairly have their ability to sue limited via the IPM, though: if the IPM were implemented, approximately 39.7 percent of Americans would be subscribed to an identity protection service to protect them from the consequences of a data breach.[206] Implementing the IPM might thus fairly prevent or limit data breach litigation involving those Americans.

In these ways, the litigation waiver envisioned by the IPM could be beneficial. Unfortunately, reducing the threat posed to employers by litigation might reduce employers' incentive to stop data breaches from occurring.

---

[204] *I.e.,* the employer would be providing the service that would provide the notifications that could conceivably allow for a workplace data breach to be detected, brought to the attention of employees, and litigated over.

[205] CAL. LAB. CODE §§ 2698-2699.5, *available at* http://bit.ly/1Isg9qa.

[206] *See supra* note 160 (119.98 million + 6.7 million=126.68 million; 126,680,000 / 318,892,103=0.3972503514770323; 0.3972503514770323 x 100=39.72503514770323).

i.2 In Each Case, Calculating Costs Based in Part On Experience Makes Sense

The potential reduction in incentives for employers to try to stop data breaches from occurring might be offset by one provision of the IPM: companies with good (1) data security systems or (2) data breach records will not pay as much for identity protection as those with lesser ones.

The former element would be similar to "cost allocation" under WC, in which more dangerous industries pay more into the WC system and less dangerous ones pay less. The latter element would be similar to WC insurance's use of "experience ratings," where companies' premiums are based on predictions about their likelihood of suffering coverable costs.[207] There is already data indicating what kinds of entities are most likely to suffer breaches.[208]

---

[207] GOETSCH, OCCUPATIONALSAFETY, *supra* note 173 at 138 (cost allocation), 145 (experience ratings).

[208] MAYER BROWN, *Trends in Data Breach and Cybersecurity Regulation, Legislation and Litigation* (Apr. 17, 2014), http://www.mayerbrown.com/files/Event/9a1f69a8-83e3-4552-aaea-a9d3b9bbea5d/Presentation/EventAttachment/28f442d0-1438-4b1c-afe2-b29cbf4aa6ef/709074307_1.pdf ("Observers believe that some industries face heightened risks, including: Healthcare / pharmaceutical[,] Financial services[,] Infrastructure

ii. Some Shortcomings of WC May Apply to the IPM, Others May Not

Thus far, positive parallels between WC and the IPM have been established. One might wonder about whether there are any negative parallels. Would costs spike due to (1) abuse of the IPM or (2) changes in technology, which undermine its utility?

ii.1 WC and the IPM Are Not Equally Ripe for Significant Abuses

Some allege that the WC system is being defrauded to significant effect via fraudulent acquisition of benefits from it without the requisite harms. It seems likely that the IPM would not facilitate such fraud.

To recognize this, one must first understand how people could seek to abuse the IPM. People could conceivably seek to abuse the IPM by falsely

---

(transportation, communications, energy)[,] Retail, hospitality, and other consumer-facing businesses[,] Technology[,] Education"); *see also*, VERIZON BUSINESS, 2009 DATA BREACH INVESTIGATIONS REPORT 6-7 (2009), http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf.

claiming to be victims of identity theft—which has happened before.[209] Or they could deliberately or negligently allow someone to steal their identities. There is reason to believe the appeal and occurrence of such actions would be limited under the IPM.

Specialized procedures exist for detecting false identity theft claims that will stop most people from successfully making such claims.[210] Those

---

[209] *E.g.,* Press Release, Department of Justice, Former California Assemblyman Admits Defrauding Banks Out Of $193,661 By Falsely Claiming To Be Identity Theft Victim (Feb. 21, 2013), http://1.usa.gov/1KyZIp8.

[210] *Identity Theft: When You Personally Know the Identity Thief*, MERCER CNTY. SHERIFF (Mar. 2002), http://www.mercercountysheriff.org/Images/identity%20theft/article5.pdf ("The credit card companies and financial institutions…know [some] people will [falsely] claim a crime was committed (stolen card or identity theft)… One of the standards they have [consequently] adopted…is that a person will probably not file a police report if they are making a false claim. It is your task to convince them that another person has [truly stolen your identity]... You will have to prove that you have not [fraudulently] benefited financially from [the resulting activities related to the theft]. Unfortunately, without a police report, your job will be much tougher."); *Credit Repair Scam Through Claim of Identity Theft*, Nat'l Credit Union Admin (Apr. 2008), *available at* http://www.ncua.gov/Resources/Pages/ FA2008-05.aspx ("[W]hen a credit report is obtained that reflects the person is a victim of identity theft[, t]hat person should be able to provide such documents as the police report they filed, the listing of disputed accounts, and the name(s) of the credit bureaus they filed with. Consideration should…be given to obtaining credit reports from more than one credit reporting agency in these situations as the perpetrator may have only attempted to "clean up" their credit report with one agency. Management must ensure they file a Suspicious Activity Report when required by established regulation… [M]anagement must provide notice to the appropriate NCUA Regional Director, and in the case of state-chartered credit unions, to their state supervisory authority.").

who are not stopped are eventually caught seemingly rather simply and quickly,[211] or otherwise because their schemes become so complicated that they implicate themselves.[212] As such, remote and rapid data monitoring is sufficient to catch the perpetrators. Close, physical surveillance is not necessary.

In addition, several factors may reduce the likelihood of people allowing themselves, or seeking, to become victims of identity theft perpetrated by others. Employees may be unwilling to behave in such ways if made aware of (1) what they (i.e. employees) will or will likely have to do to benefit from the schemes,[213] and (2) certain dangers of identity theft.[214]

In the case of all potential abuses, the following countervailing considerations can be raised. First, at least *some* policies have set noteworthy limitations to how much lost work time

---

[211] *E.g., Lyons Falls Woman Accused of Lying About Identity Theft,* WATERTOWN DAILY TIMES (Oct. 13, 2011), *available at* http://www.watertowndailytimes.com/article/20111013/NEWS07/710139932.

[212] *See, e.g., supra* note 209.

[213] *Supra* note 210 (file police report); *Your Identity Theft Plan Covers*, LEGALSHIELD, http://www.legalshield.com /legalshield-plans/identity-theft/identity-theft-plans/#idTheftPremium-more-details-lightbox (last visited May 9, 2015) (some identity theft protection services will not cover "[a]ny [s]tolen [i]dentity [e]vent where the victim is unable or unwilling to prosecute the person who caused the victim to suffer the fraud or its consequences").

[214] *Supra* note 30 (potential false implication for crimes), 73 (identity theft damage is *almost* always correctable) and accompanying text; *see also*, ROBERT W. KOLB, ENCYCLOPEDIA OF BUSINESS ETHICS AND SOCIETY 1102 (SAGE 2008) (some identity theft problems cannot be resolved).

they will pay for, and how much they will pay for it.[215] Second, there are known average times taken to resolve identity theft problems experienced by individuals with identity protection, and they are much shorter than those without identity protection.[216] Third, some identity protection services resolve nearly every aspect of the problem for the subscribers.[217] Given these considerations, an employer might demand that employees work to resolve the identity theft-related problems while at the workplace. It seems there is no reason this could not be the case, as it appears employees can already be expected to work despite facing identity theft.[218]

For these reasons, while WC may be ripe for costly abuses the IPM may well not be.

iii. 2 Costs Associated With Technological Advancements Might Be Problematic for WC and the IPM

Unfortunately, there may well be parallels

---

[215] *E.g.,* $500 per week for up to four weeks. *Identity Theft Insurance*, PRIVABLOCK, http://www.privablock.com/identity-theft-insurance.html (last visited May 9, 2015); *The Identity Defender (TM) Identity Theft Program*, U.S. LEGAL SERVICES, http://www.uslegalservices.net/legal-insurance-plans/identity-defender (last visited May 9, 2015); *Identity Protection*, PAID 2 SAVE NETWORK, http://bit.ly/1zWgkqX (last visited May 9, 2015).

[216] GLOBENEWSWIRE, *Time and Money*, *supra* note 100.

[217] MYNAMEHASBEENSTOLEN, *Ratings, supra* note 79.

[218] *See, Identity Theft Takes Its Toll On Our Workplaces*, LVB.COM (July 15, 2013), http://bit.ly/1EuAsvC.

between the costly impacts of technological developments on the IPM and WC. Costs associated with WC increased due to advancements in medicine related to technology and treatments. Costs associated with the IPM seem likely to increase continuously due to technological developments linked to the emergence of new identity theft schemes and technologies. Such schemes and technology might require new technology for, or methods of, monitoring and detecting them.[219] The increased incidence of identity theft may also play a role in potentially constant cost increases. Much like WC, perhaps this concern can be addressed by asking who is better suited to handle these increases, and who is responsible for them. With respect to both questions, given the information provided above—e.g., with respect to the Sony Pictures Entertainment data breach—the answer cannot be employees alone.

V. CONCLUSION

Data breaches are costly to the world. They

[219] *Compare*, George Tillmann, *Opinion: Stolen Fingers: The Case Against Biometric Identity Theft Protection*, COMPUTERWORLD (Oct. 27, 2009), http://bit.ly/1FYu0mf (predicting problems with theft of biometric information), *with,* Neal Ungerleider, *The Dark Side of Biometrics: 9 Million Israelis' Hacked Info Hits the Web*, FAST COMPANY (Oct. 24, 2011), http://bit.ly/1H8JX83 (the fingerprints of nearly every Israeli were stolen and sold multiple times); Iain Thomson, *German Minister Fingered As Hacker 'Steals' Her Thumbprint From A Photo*, REGISTER (Dec. 29, 2014), http://bit.ly/1An17he (noting that it is possible to make copies of retinas—not just fingerprints—via high-resolution photographs that are capable of fooling biometric-based systems).

are costly to employees as well. Presently, employees are not adequately protected from, and are often exposed to harm by workplace data breaches. While the breaches may go undetected, the employees will feel their consequences nonetheless. This needs to change to be fair to employees, but any change must also be fair to employers. The proposals in this paper are a means of accomplishing such a change for the long term, or at least until seemingly ever-elusive developments in attitudes and technology occur.