William & Mary Law Review

Volume *57 (2015-2016)*
Issue 3

Article 6

2-15-2016

Shifting Data Breach Liability: A Congressional Approach

Justin C. Pierce

NOTES

SHIFTING DATA BREACH LIABILITY: A CONGRESSIONAL APPROACH

TABLE OF CONTENTS

INTRODUCTION

Over the past several decades, consumers have increasingly relied on electronic payment systems to make purchases in stores and online.[1] In these transactions, consumers allow merchants to transmit their personal financial data among networks of banks and third-party services to verify payment.[2] Once approved, merchants give consumers the good or service in exchange for electronic payment.[3] This chain of information and storage of large amounts of personal data create an attractive target for hackers seeking to steal financial data for fraudulent purposes. Rather than physically stealing data from individual consumers one card at a time, hackers can infiltrate vulnerable computer systems and download data records containing the sensitive information of thousands of customers.

Recent incidents affecting large merchants, such as Target,[4] emphasize the growing occurrence and breadth of mass data breaches in the United States.[5] Other entities with major data breaches include T.J. Maxx/Marshalls,[6] Heartland Payment Systems,[7] Sony,[8]

---

1. *See* Catherine New, *Cash Dying as Credit Card Payments Predicted to Grow in Volume: Report*, HUFFINGTON POST (June 7, 2012, 12:47 PM), http://www.huffingtonpost.com/2012/06/07/credit-card-payments-growth_n_1575417.html [https://perma.cc/37H8-2GYK].

2. *See infra* Part I.B.

3. *See infra* Part I.B.

4. *See Data Breach FAQ*, TARGET, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888 [https://perma.cc/G7LQ-VAQ4] (last visited Feb. 21, 2016); Miles Parks, *Target Offers $10 Million Settlement in Data Breach Lawsuit*, NPR (Mar. 31, 2015, 2:58 PM), http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit [https://perma.cc/RYT5-MF8L].

5. *See Chronology of Data Breaches: Security Breaches 2005-Present*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breach [https://perma.cc/GCW5-GZUF] (last visited Feb. 21, 2016). *See generally* N. ERIC WEISS & RENA S. MILLER, CONG. RESEARCH SERV. [CRS], R43496, THE TARGET AND OTHER FINANCIAL DATA BREACHES: FREQUENTLY ASKED QUESTIONS (2014), https://www.fas.org/sgp/crs/misc/R43496.pdf [https://perma.cc/V87H-EHYS].

6. *See* Jaikumar Vijayan, *One Year Later: Five Takeaways from the TJX Breach*, COMPUTERWORLD (Jan. 17, 2008, 12:00 AM), http://www.computerworld.com/article/2538711/cybercrime-hacking/one-year-later--five-takeaways-from-the-tjx-breach.html [https://perma.cc/696P-KRHL].

7. *See* Jaikumar Vijayan, *Heartland Breach Expenses Pegged at $140M—So Far*, COMPUTERWORLD (May 10, 2010, 8:00 PM), http://www.computerworld.com/article/2518328/cybercrime-hacking/heartland-breach-expenses-pegged-at--140m----so-far.html [https://perma.

Home Depot,[9] and Anthem.[10] Although criminal actors seeking to steal information perpetrated each of these attacks, the data breaches also featured a lack of proper procedures and protections on the part of the victimized company.[11]

Data breaches, particularly those affecting millions of people, impose huge costs in the form of investigations, replacement cards, fraudulent charges, damage to merchants' reputations, and harm to consumers' privacy.[12] Of course, some party—or multiple parties—must assume financial responsibility for these damages. Currently, the liability for breach rests with each harmed party, subject to allocation by contract.[13]

In the small sample of data breaches noted above, hackers targeted the weakest link along the chain of entities that protect customer data—merchants. Because the harm from data breaches falls to each party—not just the party that failed to implement reasonable security standards—merchants do not fully realize the total costs of breach, and, therefore, merchants may underprotect customer data.

This Note proposes that Congress pass legislation to hold business entities liable for data breaches if they fail to exercise due care in protecting personal information. From that initial distribution of liability, parties could still freely contract with one another to reallocate the risk, but the baseline liability would rest with the party at fault for not adequately protecting against breach.

---

cc/8R7M-ZCD6].

8. *See* Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011, 8:55 PM), http://www.reuters.com/article/2011/04/27/us-sony-stolendata-idUSTRE73P6WB20110427 [https://perma.cc/TV9C-4PHQ].

9. *See* John Kell, *Home Depot Facing Dozens of Data Breach Lawsuits*, FORTUNE (Nov. 25, 2014, 11:10 AM), http://fortune.com/2014/11/25/home-depot-data-lawsuits/ [https://perma.cc/NX73-FWLG].

10. *See* Michael Hiltzik, *Anthem Is Warning Consumers About Its Huge Data Breach. Here's a Translation.*, L.A. TIMES (Mar. 6, 2015, 10:34 AM), http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html#page=1 [https://perma.cc/H83R-P7XV].

11. *See, e.g.*, *infra* Part I.A.

12. *See infra* Part I.B.

13. *See* Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203, 206, 209 (2008) (arguing that private contracting produces more efficient allocations of risk than government involvement).

Part I of this Note introduces background on data breaches and discusses the harms that the various parties suffer. Part II examines the current allocation of risk among parties by focusing on state and federal laws, banks' attempted litigation against merchants for recovery of damages following data breach, and private agreements between parties. Part III suggests policy goals and critical elements necessary for any effective federal legislation seeking to set a universal standard for data security. This Part in particular contends that the party responsible for failing to take adequate precautions against data breach should initially bear the risk of loss. Part IV applies the concepts of this Note to the Personal Data Privacy and Security Act of 2014 (PDPSA) to assess whether the proposed bill—or a future bill of its kind—meets the suggested policy goals and includes the essential elements outlined in Part III. Lastly, Part V anticipates overarching counterarguments that challenge the effectiveness of a congressional approach.

I. DATA BREACHES AND HARM

Over 3 billion personal records have been exposed through data breaches—including 1.1 billion records in 2014 alone.[14] These statistics show that data theft will continue to threaten electronically stored personal information at unprecedented levels until the industry implements stronger security protocols. Data breaches not only affect the party from whom information is stolen, but also many other companies and individuals that may share liability or bear the cost of breach.[15] Encouraging stronger security protocols, therefore, benefits more than just the organization taking such precautions.

---

14. RISK BASED SEC., INC., DATA BREACH QUICKVIEW: 2014 DATA BREACH TRENDS 1 (2015) [hereinafter 2014 DATA BREACH TRENDS], https://www.riskbasedsecurity.com/reports/2014-YEDataBreachQuickView.pdf [https://perma.cc/YKV7-GKZJ]. By the third quarter of 2015, over 350 million additional records have been exposed through data breaches. RISK BASED SEC., INC., DATA BREACH QUICK VIEW: THIRD QUARTER 2015 DATA BREACH TRENDS 1 (2015) [hereinafter THIRD QUARTER 2015 DATA BREACH TRENDS], https://www.riskbasedsecurity.com/reports/2015-Q3DataBreachQuickView.pdf [https://perma.cc/65VR-NNYE].

15. *See infra* Part I.C.

A. The Target Data Breach

Though data breaches can occur through a multitude of attack schemes, this Note focuses on hacking, which accounted for 83.3 percent of records exposed in 2014.[16] The data breach at Target serves as a representative incident of hackers infiltrating a large company that stored vast amounts of consumer data—perhaps without adequate protection.

The Target data breach, revealed in December 2013, ranked number eight on the list of all-time data breaches, with over 110 million compromised records.[17] Hackers obtained "40 million credit and debit card account numbers ... [and] the names, addresses, phone numbers, and email addresses of up to 70 million consumers."[18] The hackers first obtained credentials from a third-party vendor through an email phishing scheme.[19] With the credentials, the hackers accessed a portion of Target's system and remotely installed malware on the point-of-sale registers.[20] The malware copied payment information directly from the register before it was encrypted, thereby avoiding the need to decrypt the data.[21]

Critics suggest that a third-party vendor should never have possessed credentials capable of accessing the point-of-sale system—instead, the two electronic functions should have been partitioned to prevent unauthorized access.[22] Beyond the initial security flaws that allowed access to the system, Target also did not immediately respond to early warnings that personal data could be at risk.[23] Instead, Target responded a month later, and only when contacted by the Department of Justice about suspicious payment activity.[24]

---

16. 2014 DATA BREACH TRENDS, *supra* note 14, at 3. By the third quarter of 2015, hacking accounted for 83.2 percent of the records exposed that year. THIRD QUARTER 2015 DATA BREACH TRENDS, *supra* note 14, at 1.

17. 2014 DATA BREACH TRENDS, *supra* note 14, at 10.

18. WEISS & MILLER, *supra* note 5, at i.

19. *Id.*; Brian Krebs, *Target Hackers Broke in via HVAC Company*, KREBS ON SEC., https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ [https://perma.cc/QF6K-7NCW] (last updated Feb. 14, 2014).

20. WEISS & MILLER, *supra* note 5, at i; Krebs, *supra* note 19.

21. WEISS & MILLER, *supra* note 5, at 2.

22. *See, e.g.*, Krebs, *supra* note 19.

23. *See* WEISS & MILLER, *supra* note 5, at 2.

24. *Id.* at 3.

B. The Payment Transaction Process

The Target example demonstrates one potential avenue by which hackers can attack a merchant's stored information. More importantly, the Target breach is emblematic of the inherent problems with the current allocation of liability.

Because merchants necessarily share financial data with a number of other entities to perform a transaction, a data breach can occur at any of the various entities. In these instances, the fault may not rest with a merchant, but perhaps with a financial institution or processing company, both of which could also be vulnerable to electronic attacks. An explanation of the typical credit card transaction helps one to understand the multitude of companies that must access and protect consumer information. It also highlights the stakeholders that must ensure secure payment transactions in order to avoid liability for wrongdoing.

The typical transaction begins at a retail location where the consumer swipes their card using a point-of-sale system.[25] A payment processing service communicates the data on the magnetic strip of a consumer's credit card from the merchant to the merchant's bank, known as the acquiring bank.[26] The acquiring bank then contacts the consumer's bank, known as the issuing bank, through a payment card company, such as Visa.[27] The issuing bank ensures that the consumer's account can accept a charge.[28] Once the issuing bank accepts or denies the request, it sends a response back to the acquiring bank through the payment card company.[29] Through the payment processing company, the acquiring bank conveys the message to the retail location, where the transaction is

25. *See id.* at 8.

26. *See id.* at 7-8; Epstein & Brown, *supra* note 13, at 207-08; Mark MacCarthy, *Government and Private Sector Roles in Providing Information Security in the U.S. Financial Services Industry*, 8 I/S: J.L. & POL'Y FOR INFO. SOC'Y 242, 246-47 (2012).

27. *See* WEISS & MILLER, *supra* note 5, at 8; Epstein & Brown, *supra* note 13, at 207-08; MacCarthy, *supra* note 26, at 246-47.

28. *See* WEISS & MILLER, *supra* note 5, at 8; Epstein & Brown, *supra* note 13, at 207-08; MacCarthy, *supra* note 26, at 246-47.

29. *See* WEISS & MILLER, *supra* note 5, at 8; Epstein & Brown, *supra* note 13, at 207-08; MacCarthy, *supra* note 26, at 246-47.

approved or declined.[30] If approved, the consumer walks away with the merchandise, and the store receives a promise of payment from the acquiring bank once the money is advanced by the issuing bank.[31] The consumer then repays the issuing bank after receiving his or her monthly statement of charges.[32]

Not all transactions require a payment processing company to facilitate communication, but the basic structure above demonstrates the complexity of a seemingly simple transaction. At any point during the information exchange, one of the entities could suffer an attack and allow a breach of consumer data; thus, consumer data protections work only as well as the least secure link in the chain. Just as this Note narrows its focus to attacks by hacking, it also will consider only breaches that occur through the merchant's access to consumer information. The goal, then, would be to ensure that the merchant has adequate incentives to avoid being a weak link.

C. Parties Harmed by Data Breaches

Data breaches impose costs on a number of parties that participate in the transaction process. For the purposes of this Note, the consequences that merchants and issuing banks face are most important.[33]

---

30. *See* WEISS & MILLER, *supra* note 5, at 8; Epstein & Brown, *supra* note 13, at 207-08; MacCarthy, *supra* note 26, at 246-47.

31. *See* WEISS & MILLER, *supra* note 5, at 8; Epstein & Brown, *supra* note 13, at 211; MacCarthy, *supra* note 26, at 246-47.

32. *See* WEISS & MILLER, *supra* note 5, at 8; Epstein & Brown, *supra* note 13, at 207-08; MacCarthy, *supra* note 26, at 246-47.

33. Harm to consumers largely consists of inconvenience. Although stolen financial data may lead to fraudulent charges made through the consumer's account, Congress has limited the maximum amount of fraudulent charges that an issuing bank can pass along to its consumers to $50 for credit cards and $0 to $500 for debit cards, depending on when the consumer reports the fraud. 15 U.S.C. §§ 1643(a), 1693(g) (2012); WEISS & MILLER, *supra* note 5, at 11. In practice, almost all issuing banks offer fraud monitoring services, identity theft protection, and zero fraud liability as features of a consumer's card. *See* John Kiernan, *2015 Fraud Liability Study: Which Cards Protect You Best?*, CARDHUB, http://www.cardhub.com/edu/fraud-liability-study/ [https://perma.cc/8CEL-CDGV] (last visited Feb. 21, 2016). Because of these protections, consumers seldom pay for any fraudulent charges. Aside from the financial liability, consumers have the inconvenience of reporting fraud, obtaining a new card, and perhaps worrying about an increased likelihood of future fraud or identity theft. *Id.* Compared with the financial effects passed along to issuing banks, these costs are nominal. *See infra* Part I.C.2.

1. Merchants

Merchants that suffer a data breach face more significant consequences than their customers. Following a breach, merchants typically hire cyber-security experts to evaluate the cause of the breach and secure any vulnerabilities.[34] Additionally, the merchant must navigate public relations concerns, private penalties incurred by contract, and potential regulatory violations for failing to meet minimum security standards.[35] Loss of consumer confidence could also prove detrimental to the merchant in the short term.[36] For example, Target responded to consumer concerns regarding the leaked information by offering a 10 percent discount in stores on December 21 and 22, one week after the breach occurred.[37] Issuing banks may also impose chargebacks on fraudulent purchases, meaning the merchants would not receive payment for merchandise that they mistakenly allowed an individual to fraudulently purchase.[38] In most cases, merchants will not be responsible for chargebacks if the consumer presented a physical card to make the purchase.[39] On the other hand, online and over-the-phone payments are more difficult to verify and, therefore, banks place a greater burden on merchants to accept such payments at their own risk.[40]

2. Issuing Banks

Issuing banks bear heavy expenses as a result of data breaches. These institutions must identify and investigate fraudulent activity

34. WEISS & MILLER, *supra* note 5, at 5-6; ONLINE TR. ALL., 2015 DATA PROTECTION & BREACH READINESS GUIDE 17-20 (2015), https://otalliance.org/system/files/files/resource/documents/dpd_2015_guide.pdf [https://perma.cc/9NB6-6XSY].

35. *See* WEISS & MILLER, *supra* note 5, at 16-17; ONLINE TR. ALL., *supra* note 34, at 17-20.

36. *See* ONLINE TR. ALL., *supra* note 34, at 6.

37. Victor Luckerson, *Target Gives Shoppers 10 Percent Off This Weekend*, TIME (Dec. 20, 2013), http://business.time.com/2013/12/20/target-gives-shoppers-10-percent-off-this-weekend/ [https://perma.cc/58XB-EEK3].

38. WEISS & MILLER, *supra* note 5, at 9-10.

39. *See* Robert Berner & Adrienne Carter, *The Truth About Credit-Card Fraud*, BLOOMBERG BUS. (June 20, 2005), http://www.businessweek.com/stories/2005-06-20/the-truth-about-credit-card-fraud [https://perma.cc/CVP3-G6P9]. See *infra* note 107 for a discussion on the implementation of EMV card technology that shifted liability on October 1, 2015.

40. *See* Berner & Carter, *supra* note 39.

to determine when the bank must issue new cards to consumers.[41] Even though a merchant's vulnerability may have caused the breach, issuing banks usually serve as the first line of defense for confused consumers who want to learn more about the security of their information.[42]

In addition to the costs associated with identifying and processing fraud, issuing banks also pay to issue new cards, which average around $10 per card.[43] Smaller banks spend a much higher amount than larger banks when issuing new cards, so breaches create a disproportionate effect on banks based on size.[44] Banks also typically suffer losses based on fraudulent charges—surveyed banks estimated that the Target breach resulted in an average loss of $331 per affected debit card and $530 per affected credit card.[45] In general, most banks, particularly smaller institutions with assets of less than $1 billion, have received little to no reimbursement for these breach-related expenses.[46] Without an adequate means to recoup

41. WEISS & MILLER, *supra* note 5, at 18.

42. *See* BENCHMARKING & SURVEY RESEARCH, AM. BANKERS ASS'N, TARGET BREACH IMPACT SURVEY 13-14 (2014), http://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf [https://perma.cc/U6MH-4DQ5]. One bank employee provided a narrative account of how the Target data breach impacted his institution:

> Public news of the Target data breach broke at the same time Bank began receiving lists of potentially compromised cards from our processor. This news generated the largest consumer reaction I have experienced to any event in my 22 years at this Bank. Bank phones rang, literally, non-stop for the first few business days following the public announcement. Handling and responding to these calls consumed a majority of Bank resources during this time. Callers were alarmed and very concerned about the safety of their accounts and personal information. Many consumers requested to have new debit cards issued to them even if their card had not been identified as potentially compromised in the data breach.

Id. at 14. In this case, the bank, rather than the merchant itself, bore the cost of responding to the breach, thus expending significant resources. *See id.*

43. *See* WEISS & MILLER, *supra* note 5, at 17; BENCHMARKING & SURVEY RESEARCH, *supra* note 42, at 12 ("[I]ncluded are costs for mailing, card stock, and additional staff resources, etc.").

44. BENCHMARKING & SURVEY RESEARCH, *supra* note 42, at 11 (comparing average replacement costs of $12.75 per credit card for banks holding less than $1 billion in assets with average replacement costs of $2.99 per card for banks holding $50 billion or more in assets).

45. *Id.* at 10.

46. *See id.* at 17-21 (providing survey responses from small banks affected by the Target breach).

losses, issuing banks bear a huge burden of liability with little hope of recovery from the merchants ultimately at fault.[47]

II. SHIFTING THE COST OF DATA BREACHES

Despite the national reach of many merchants and issuing banks, the United States does not currently operate under a uniform standard for data security.[48] Instead, litigants must look to the laws within individual states to determine minimum data protection standards, notification requirements, and burden-shifting mechanisms to recover damages resulting from a data breach.[49]

A. Federal Data Security Standards

The Federal Trade Commission (FTC) has led the most successful federal effort to regulate data security by bringing cases under the theory that a "failure to maintain reasonable security is an unfair practice under the section 5 of the FTC Act."[50] Specifically, in response to the BJ's Wholesale data breach, the FTC alleged that:

> Respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice.[51]

The FTC has alleged inadequate data protection using data security requirements that mirror the Data Security Standard (DSS) set by the Payment Card Industry (PCI), a private organization designed

---

47. *See* MacCarthy, *supra* note 26, at 247.

48. Ieuan Jolly, *Data Protection in United States: Overview*, PRAC. L., http://us.practicallaw.com/6-502-0467 [https://perma.cc/3JY8-8MWM] (last updated July 1, 2015).

49. *See id.*

50. MacCarthy, *supra* note 26, at 251; *see also* John P. Hutchins & Renard C. Francois, *A New Frontier: Litigation over Data Breaches*, 10 PRAC. LITIGATOR 47, 48-50 (2009).

51. Complaint at 3, *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005) (No. C-4148), http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf [https://perma.cc/NXM7-9F8D].

to set industry standards for credit card transactions.[52] Importantly, the FTC's reference to the PCI DSS supports the argument that the PCI DSS represents a de facto legal duty in the payment industry.[53] As such, companies may seek to comply with PCI DSS requirements to avoid liability.[54] The FTC model also illustrates that a federal standard could simply reflect evolving industry norms, as developed by a private organization.[55]

B. State Data Security Standards

State law factors into the equation much more heavily than federal law. Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have passed laws that require companies to notify parties affected by a data breach involving personally sensitive information.[56] These laws set a static condition that triggers a duty: companies must notify customers about data breaches involving personal financial information once the breach has occurred.[57] The statutes do not set or encourage industry standards to actually prevent data breaches.[58] Instead, these limits require

52. MacCarthy, *supra* note 26, at 251; *see also* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES (2015), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf [https://perma.cc/PY4L-QN9K] [hereinafter PCI STANDARDS]. For a discussion of the PCI DSS, see *infra* Part II.C.

53. *See* MacCarthy, *supra* note 26, at 251-52. *See generally* Hutchins & Francois, *supra* note 50.

54. *See* MacCarthy, *supra* note 26, at 251-52.

55. *See id.*

56. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (June 11, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/R9ZT-X5UY]. The NCSL makes clear that:

> Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of 'personal information' (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

Id.; *see also* GINA STEVENS, CRS, R42475, DATA SECURITY BREACH NOTIFICATION LAWS 5-6 (2012), https://www.fas.org/sgp/crs/misc/R42475.pdf [https://perma.cc/BB8Y-X46W] (discussing the different elements of security breach notification laws).

57. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 319 (2014).

58. *See id.* at 320-21.

breached entities to share information about the data breach to prevent unnecessary harm caused by delayed reporting.[59]

Some have criticized security breach notification statutes for creating safe harbors that allow entities to avoid liability merely by meeting certain requirements, such as encrypting data.[60] One Chief Information Security Officer (CISO) of a major healthcare company commented on the effect of the security breach notification laws: "[N]otification laws ... have essentially reversed the whole direction security was taking.... [S]ecurity investment is moved essentially to crypto. Just encrypt as much as you can. Whatever it takes, just encrypt it. If it moves, encrypt it. If it stays there, encrypt it."[61]

Encouraging companies to implement effective data security protocols certainly meets policy objectives, but a problem arises if companies allocate funding to comply with safe harbors rather than actually implementing measures to make the system reasonably secure. As the statute ages, a once useful data protocol will become outdated and virtually useless.[62]

In addition to notification statutes, thirty-one states and Puerto Rico have passed data disposal laws that require "entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable."[63] These laws seek to prevent theft of private financial information by limiting the information that entities store on their servers.[64]

Massachusetts, which has enacted both notification and disposal statutes,[65] encourages businesses to follow the PCI DSS; for example, consent judgments have required companies to "maintain PCI DSS compliance, or such compliance standards that may be from time to time recognized by the payment card industry as acceptable."[66] Though not codified, this case law indicates that

59. Hutchins & Francois, *supra* note 50, at 49.

60. *See* Thaw, *supra* note 57, at 322.

61. *Id.* at 321.

62. *See* MacCarthy, *supra* note 26, at 253.

63. *Data Disposal Laws*, NAT'L CONF. ST. LEGISLATURES (Jan. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx [https://perma.cc/L9N8-ET53].

64. *See id.*

65. MASS. GEN. LAWS ANN. ch. 93H, § 3 (West 2015); *id.* at ch. 93I, § 2.

66. Final Judgment by Consent at 4, Commonwealth v. Briar Grp., LLC, Civ. No. 11-1185B (Mass. Super. Ct. Mar. 28, 2011); *see also* MacCarthy, *supra* note 26, at 252 (discussing Massachusetts's efforts to incorporate the PCI DSS into its enforcement).

Massachusetts supports enforcement of the PCI standards and seeks to allow the Commonwealth's standards to evolve with the industry over time.[67]

Minnesota, the state where issuing banks brought suit against Target,[68] follows a different approach. Rather than follow the evolving PCI standard, the legislature incorporated specific elements of the PCI DSS into its state law.[69] This approach could present problems as the industry standard changes and the statute remains the same—potentially creating a conflict between the industry's best practices and outdated state law.[70] If an entity suffers a data breach while not complying with the statute, the law holds the entity liable for consequential damages, including the harms suffered by issuing banks.[71] Although the enforcement of a mandated data security standard and the availability of consequential damages currently makes Minnesota one of the best defenders of data security, the approach could have negative long-term effects if the state standard becomes outdated.[72]

The inconsistent state and federal standards—or lack thereof—make data breach litigation difficult to predict on a national scale. In practice, the variety of standards creates a need for litigation, which makes recovery difficult, if not impossible, for issuing banks—particularly for smaller institutions with limited resources that may not be capable of challenging a larger merchant. Furthermore, state notification statutes demonstrate the potential dangers of creating rigid exceptions to liability that cannot evolve over time.

C. Private Card Industry Data Security Standards

In 2006, American Express, Discover Financial Services, JCB International, MasterCard, and Visa, Inc. formed the Private Card Industry (PCI) Security Standards Council (SSC) to promote "development, management, education, and awareness of the PCI

67. *See* MacCarthy, *supra* note 26, at 252.

68. *See In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014).

69. MINN. STAT. § 325E.64 (2014); *see also* MacCarthy, *supra* note 26, at 252 n.24.

70. *See* MacCarthy, *supra* note 26, at 252-53.

71. Epstein & Brown, *supra* note 13, at 221.

72. *See* MacCarthy, *supra* note 26, at 252-53.

Security Standards."[73] Member processing card companies require users to agree to the Security Standards (PCI DSS) by contract in order to issue cards (issuing banks) or accept payments (acquiring banks and payment processing companies).[74] In addition, these agreements require acquiring banks to obtain a guarantee that *merchants* working with the bank will comply with the PCI DSS as well.[75] Thus, the PCI Council effectively sets a minimum data security standard for all stakeholders in the industry as a condition on using the card service.[76] The PCI DSS helps to distribute the risk issuing banks hold by allocating liability to merchants, acquiring banks, and payment processors based on non-compliance with the required data security standards.[77]

The PCI DSS sets an industry standard by requiring twelve basic protections for all users handling financial data. Users must:

> 1. Install and maintain a firewall configuration to protect cardholder data
> 2. [Refrain from using] vendor-supplied defaults for system passwords and other security parameters
> 3. Protect stored cardholder data
> 4. Encrypt transmission of cardholder data across open, public networks
> 5. Protect all systems against malware and regularly update anti-virus software or programs
> 6. Develop and maintain secure systems and applications
> 7. Restrict access to cardholder data by business need to know
> 8. Identify and authenticate access to system components
> 9. Restrict physical access to cardholder data
> 10. Track and monitor all access to network resources and cardholder data
> 11. Regularly test security systems and processes

---

73. *About Us*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/organization_info/index.php [https://perma.cc/JZ7B-DP26] (last visited Feb. 21, 2016).

74. MacCarthy, *supra* note 26, at 249-50; PCI STANDARDS, *supra* note 52, at 12.

75. MacCarthy, *supra* note 26, at 249.

76. *See* Hutchins & Francois, *supra* note 50, at 53 ("A company processing, storing, or transmitting payment card data must be PCI-DSS compliant or risk losing their ability to process credit card payments and being audited and/or fined.").

77. *See* MacCarthy, *supra* note 26, at 248.

> 12. Maintain a policy that addresses information security for all personnel.[78]

Each of these requirements seeks to regulate the information that entities maintain and implement procedures to protect that retained information. The twelve practices outlined by the PCI also serve as a model of industry best practices for other organizations, courts, and legislatures.[79]

The PCI standards incentivize all parties to consider the potential costs associated with data breaches.[80] Depending on an individual state's contract law, however, parties can have difficulty applying the agreed-upon standards consistently.[81] Issuing banks, for example, still have trouble recovering damages from merchants even when all members have agreed to follow the same PCI data standard.[82]

D. Litigation by Issuing Banks

Data breaches occur when hackers steal mass amounts of consumer information from company servers, but most hackers never face prosecution.[83] Even if investigators could discover these criminals and hold them liable, those criminals would not have the financial resources to compensate the parties harmed by the breach. In the absence of holding the criminal actor liable, litigants must look to another party for compensation.

In cases in which a merchant's inadequate security protocols resulted in a data breach, consumers and issuing banks have attempted to shift the damages they suffered back to the merchant responsible for the breach.[84] Pointing the finger at the merchant

---

78. PCI STANDARDS, *supra* note 52, at 5.

79. *See* MacCarthy, *supra* note 26, at 273 ("[The] PCI [Security Standards Council] is heavily involved in the development of information security standards.").

80. *See id.* at 254-55.

81. *See infra* Part II.D.

82. *See infra* Part II.D.

83. *See* Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1180-81 (2014) (discussing the difficulty that the United States and other countries have in prosecuting cyber-crimes).

84. *See* Hutchins & Francois, *supra* note 50, at 50-53 (summarizing recent examples of private litigation against merchants for breaches of consumer data).

may seem unfair because, after all, the merchant also fell victim to the theft, but the merchant collected volumes of valuable information in one location and then essentially left the vault open, the door unlocked, or the key under the mat. Issuing banks—especially smaller institutions that struggle to bear the cost of data breaches—have attempted to recover damages from merchants following data breaches.[85] As in other consumer litigation, issuing banks have argued under negligence, breach of contract, and state law theories.[86]

1. Negligence

As plaintiffs, issuing banks may succeed in demonstrating damages, causation, and breach of a reasonable standard of care based on the merchant's noncompliance with contractual obligations to third parties or with a statutory requirement. Banks have nonetheless struggled to show that merchants owed them a duty because the issuing bank and merchant have no direct connection.[87] To overcome this challenge, issuing banks have tried to argue that a special relationship between the parties creates a common law duty.[88] Courts, however, have been reluctant to recognize a special relationship that would create a common law duty.[89]

---

85. *See, e.g.*, Plaintiff's Memorandum in Opposition to Defendant's Motion to Dismiss at 1, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. Oct. 1, 2014) (No. 14-2522), ECF No. 204 (naming plaintiffs, including five financial institutions: Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain).

86. Many consumers have attempted to raise class action claims against merchants for failing to protect payment information. *See generally* 3 E-COMMERCE AND INTERNET LAW § 27.07, Westlaw (database updated Dec. 2014). Consumers attempt to bring claims based on the inconvenience of the breach or increased likelihood of future identify theft. *See id.* Courts generally dismiss consumer claims because plaintiffs fail to establish any injury as a result of the data breach because the issuing banks assume financial liability. *See id.* In some cases, consumers establish constitutional standing but then fail to demonstrate injury as the negligence claim requires. *See id.* The legal theories have included negligence, breach of an implied contract, and statutory relief derived from various state laws. *See id.* This Note does not, however, discuss the legal remedies available to consumers.

87. *See, e.g.*, *In re* Sony Gaming Networks and Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012); Elavon, Inc. v. Cisero's Ristorante, Inc., No. 100500480, 2013 WL 8215464, at *4 (Utah Dist. Ct. Mar. 21, 2013).

88. *See* BancFirst v. Dixie Rests., Inc., No. CIV-11-174-L, 2012 WL 12879 (W.D. Okla. Jan. 4, 2012).

89. *See id.* at *4 ("[Merchant]'s responsibilities under the PCI Data Security Standards reflect that these are general obligations that apply to all cardholders and banks, whether

Even if plaintiffs survive the initial challenge of establishing the prima facie case, merchants have successfully defended against liability by asserting the economic loss doctrine.[90] The doctrine varies from state to state and therefore offers different protection depending on jurisdiction.[91]

2. Breach of Contract

Under a breach of contract theory, issuing banks assert that a contract between a merchant and the acquiring bank (or acquiring

---

issuing or acquirer. The obligations are not specific to [the plaintiff issuing bank] and do not create a special responsibility by [the merchant] to [the issuing bank]."); *see also* Defendant's Memorandum of Law in Support of Motion to Dismiss the Consolidated Class Action Complaint at 6-7, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014) (No. 14-2522), ECF No. 183 (arguing that plaintiffs' negligence claim should be dismissed for failing to establish that a "special relationship" existed).

90. *See, e.g.*, Cotton Patch Café, Inc. v. Micro Sys., Inc., No. MJG-09-3242, 2012 WL 5986773, at *5 (D. Md. Nov. 27, 2012).

91. *See* Banknorth, N.A. v. BJ's Wholesale Club, Inc., 394 F. Supp. 2d 283, 287 (D. Me. 2005) ("Not all states have adopted the economic loss rule, and those that have vary widely in their understanding of the doctrine's scope."); *see also* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 423 (5th Cir. 2013) (examining how Texas and New Jersey differ in their respective application of the economic loss doctrine). Applying New Jersey law, the court in *Lone Star National Bank*, while adjudicating the Heartland Payment Systems data breach, quoted the New Jersey Supreme Court on the purpose of the economic loss doctrine:

> Generally speaking, tort principles, such as negligence, are better suited for resolving claims involving unanticipated physical injury, particularly those arising out of an accident. Contract principles, on the other hand, are generally more appropriate for determining claims for consequential damage that the parties have, or could have, addressed in their agreement.

Lone Star Nat'l Bank, 729 F.3d at 424 (quoting Spring Motors Distribs., Inc. v. Ford Motor Co., 489 A.2d 660, 671-72 (N.J. 1985)). The Fifth Circuit reversed the District Court's granting of a motion to dismiss based on four findings. *Id.* at 426. First, the issuing banks constituted an identifiable class. *Id.* Second, the claim would not impose limitless liability on the payment processor (here, the payment processor suffered the data breach, not a merchant). *Id.* Third, absent negligence there would be no other remedy for the issuing banks. *Id.* Fourth, it is not clear whether the parties could have actually negotiated terms with one another because they did not have a direct connection. *Id.*

The economic loss doctrine does not appear to be an issue in the Target litigation, applying Minnesota law. *See* Plaintiff 's Memorandum in Opposition to Defendant's Motion to Dismiss the Consolidated Class Action Complaint at 26-27, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. Oct. 1, 2014) (No. 14-2522), ECF No. 204 ("Minnesota's economic loss doctrine ... has been highly circumscribed by statute ... and has no bearing on [the issuing banks]' negligence claim (Target, tellingly, has not argued otherwise).") (citation omitted).

bank and payment/card processor) specified a minimum level of data security and the merchant breached that contract by allowing hackers to exploit a vulnerable system.[92] Issuing banks must then persuade the court to recognize the issuing bank as a third-party beneficiary to the contract, thus allowing them to bring a breach of contract claim.[93]

Applying Pennsylvania law, the Third Circuit left open the possibility of such an argument.[94] The court concluded that in order to be an intended beneficiary of the member agreement (between the payment card company and the acquiring bank), the issuing bank must prove that the payment card company intended to give the issuing bank the benefit of the acquiring bank's promise to ensure that the merchant would comply with the provision of the member agreement prohibiting merchants from retaining cardholder information.[95]

The issuing banks' various legal strategies demonstrate the problem created by the lack of uniform law outlining liability for data breaches. Merchants operating throughout the country face varying liability based on the states in which an issuing bank may find proper jurisdiction and venue for a claim. For the banks, the patchwork system means that the institution cannot always—or even often—recover damages resulting from the merchant's data breach. Congress should correct these inconsistencies by implementing a uniform allocation of liability between merchants and issuing banks.

III. GUIDELINES FOR FEDERAL LEGISLATION

Creating a uniform security standard, rather than requiring an interpretation of fifty separate state law practices, would help companies that store consumer information better evaluate their potential liability.[96] Entities can then take concrete steps toward

92. *See, e.g.*, Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 168 (3d Cir. 2008).

93. *See id.* at 168, 172.

94. *See id.* at 173.

95. *Id.* at 172.

96. *See* Thaw, *supra* note 57, at 361.

compliance with one data security standard that, if followed, will protect them from liability.

Congress should draft federal legislation designed to: (1) reduce the occurrence of data breaches by allocating liability to the breached party (merchants for this Note); (2) evolve with industry standards to avoid outdated and ineffective requirements; and (3) minimize consequential harm by requiring notification following a data breach. In carrying out these three objectives, Congress would protect consumers and issuing banks while encouraging better merchant practices.

A. Prevention Through Allocation of Liability

Congress should incentivize merchants to take greater precautions to protect sensitive data. Generally, risk can be best mitigated by assigning liability to the party in the best position to avoid the harm.[97] In the case of data breaches, many different parties along the chain of information could be responsible for a data breach. Hackers may choose to target larger entities to obtain a large amount of information at once or look for the party with the most vulnerable system protocols. The current distribution of liability—in which consumers and issuing banks cannot recover damages from merchants—prevents merchants from fully realizing the harm caused by inadequate standards.[98]

Instead, Congress should place liability with the breached party (the merchant for the purposes of this Note) if that entity failed to comply with the requisite data security standards. For companies that fully comply with data security standards and yet still suffer a breach—because hackers will continue to engage in criminal activity—the statute would not shift liability. Rather, each party would be responsible for their own harms, as under the current system.

Although the FTC's current practice to extend the PCI DSS through federal enforcement has proven successful, it stops short of

---

97. *See* Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L.J. 1055, 1060-62 (1972) (explaining the "cheapest cost avoider").

98. The same could be said of issuing banks or payment processors. Because each party currently bears certain costs based on their role in the transaction, rather than their role in the data breach, they do not have to account fully to one another. *See* MacCarthy, *supra* note 26, at 248.

providing remedies to harmed parties—such as issuing banks.[99] Private contract has also failed to encourage adequate data security or remedies for issuing banks.[100] Therefore, many institutions harmed by merchants' failures to meet the minimum PCI security standards must bear their own costs.[101] A federal statute shifting the burden to the breached party would expand the current FTC enforcement regime to protect parties harmed by entities' failures to maintain proper data security protocols.

Merchants are in the best position to prevent attacks against their own systems, so they should bear liability for those data breaches that occur due to a lack of reasonable security. In order to reduce vulnerability, merchants can implement stronger technology systems, employ monitoring services, and maintain regular testing on the system—basically, merchants could fully embrace the PCI DSS.[102] Issuing banks, in contrast, can do very little to protect information stored by the merchant. Thus, issuing banks should not be held accountable for breaches resulting from poor data management on the part of the merchant.[103]

Some argue that shifting additional liability to the merchants would not achieve any beneficial results because the PCI already pressures merchants to follow proper procedures in order to avoid hefty fines.[104] Therefore, the harm merchants currently suffer following a data breach may already be enough to incentivize compliance. For example, estimates indicate that Target may lose more than $1 billion as a result of the breach, not to mention harm from lost sales, damage to its reputation, and other costs merchants bear.[105] Nonetheless, data breaches continue to occur at an unprecedented rate, and holding the breached party responsible for

99. *See id.* at 251; *see also* Hutchins & Francois, *supra* note 50, at 49-50.

100. *See* MacCarthy, *supra* note 26, at 249-50 (doubting the effectiveness of a private contract model, such as PCI DSS, to remedy the problem of data breaches fully on its own).

101. Hutchins & Francois, *supra* note 50, at 54.

102. *See* PCI STANDARDS, *supra* note 52, at 5, 13-14 (discussing "best practices" to comply with PCI DSS requirements and the effect such compliance would have on payment system vulnerability).

103. *See* MacCarthy, *supra* note 26, at 269. *But see infra* note 107.

104. *See* Epstein & Brown, *supra* note 13, at 216 (noting that PCI already allows processing card companies to fine merchants for noncompliance. For example, Visa assesses penalties up to $100,000 per incident and $500,000 per incident if the merchant was noncompliant).

105. WEISS & MILLER, *supra* note 5, at 6, 14-17, 19; *see supra* Part I.C.1.

maintaining a vulnerable system may be the most efficient way to combat the problem.

Another option would be to assign liability to the issuing banks or maintain the current allocation, which also essentially has the effect of placing liability on issuing banks.[106] Financial institutions may not be in the best position to prevent data breaches, but perhaps they are in the best position to manage risk of liability. If the transaction costs of issuing credit cards becomes too high, banks will pass along these costs to their customers by raising rates and charging additional fees to meet target margins. Banks could also implement new card technology to make transactions safer or implement procedures to make transactions more difficult, either of which could reduce the risk of fraud.[107] Smaller banks would likely suffer most from this approach, as they do under the current system, because they have neither the same resources to mitigate fraud nor the same elasticity to bear the brunt of liability in the face of mass data breaches.[108]

---

106. Alternatively, Congress could allocate liability to consumers. Since consumers could not afford to bear substantial losses resulting from fraud, they would be strongly incentivized to conduct business only with trusted merchants and to protect the physical security of their information. *See* Epstein & Brown, *supra* note 13, at 206. The majority of data breach crimes occur, however, by hacking trusted merchants, suggesting that the average consumer could do very little to protect themselves. *See* MacCarthy, *supra* note 26, at 268-69. Such a shift also seems highly unlikely considering that consumer-friendly legislation has traditionally protected consumers from potential harm. *See supra* note 33.

107. *See* WEISS & MILLER, *supra* note 5, at 10-12 (suggesting that issuing banks should implement "chip" credit cards that would prevent a substantial amount of the fraud caused by data breaches). Most credit card companies announced that liability for fraud would shift to the entity not using EMV chips (whether the merchant or the bank) on October 1, 2015. *See e.g.*, Press Release, Visa, Visa Announces U.S. Participation in Global Point-of-Sale Counterfeit Liability Shift (Aug. 9, 2011), http://usa.visa.com/download/merchants/bulletin-us-participation-liability-shift-080911.pdf [https://perma.cc/VSU9-5YVR]; Cathy Medich, *EMV Migration—Driven by Payment Brand Milestones*, EMV CONNECTION, http://www.emv-connection.com/emv-migration-driven-by-payment-brand-milestones [https://perma.cc/2XPF-P878] (last visited Feb. 21, 2016). Despite the recent shift, many doubt whether merchants and banks are ready for the change. *See* Samantha Masunaga, *Some Small Businesses Still Unsure About Credit Card Chip Technology*, L.A. TIMES (July 28, 2015, 2:51 PM), http://www.latimes.com/business/la-fi-card-readers-20150728-story.html [https://perma.cc/3B4B-WV79].

This suggests that holding issuing banks liable for some share of the consequential damages following a data breach acts as an incentive for the bank to minimize fraudulent activity. Otherwise, the bank could allow continued charges at the expense of the merchant responsible for the data breach.

108. *See supra* Part I.C.2.

Merchants, therefore, are in the best position to avoid the harm that all parties will suffer as a result of data breaches. Although issuing banks may be capable of bearing the liability, such an allocation would not help to alleviate the overall economic strain posed by the underlying problem. By incentivizing merchants to implement strong data security protocols, Congress will help to reduce the overall incidence of data breaches and protect consumer information.

B. Evolving Standards Based on the PCI DSS

Successful federal legislation depends on implementing a uniform data security standard that can evolve over time based on industry standards and changing technology. A dynamic standard will require entities to constantly maintain adequate levels of data protection rather than rely simply on compliance with a set, static standard in order to avoid liability.[109] Because the private sector has already developed a widely used and accepted standard that changes based on industry needs, Congress could rely on the PCI DSS when creating federal requirements.[110]

Despite its high degree of predictability, codifying a particular set of data security requirements would cause problems because the codified standards could not adapt to changing industry standards.[111] Similar to the Minnesota statute that codified the PCI standard in part, this approach would become outdated over time and, perhaps more importantly, create a conflict between federal law and industry best practices.[112] In the latter scenario, entities could shield themselves from liability by complying with baseline security protocols while still remaining vulnerable to hackers. As previously noted, static provisions in a codified standard, such as data encryption, could also create safe harbors that may prevent companies from using their resources efficiently to prevent

109. MacCarthy, *supra* note 26, at 268-69.
110. *Id.* at 274.
111. *Id.* at 253, 275.
112. *Id.* at 252-53.

breach.[113] Rather, companies will look to avoid liability without developing new strategies.[114]

Instead, Congress should implement an evolving standard based on the existing PCI DSS standard. Deference to the private sector on forming a data security standard has many benefits. Congress would not have to start from scratch in order to create a universal standard, nor would it need to expend resources updating the promulgated standard over time.[115] Private industry may also be in a better position to determine the best practices for protecting consumer information.[116] Federal legislation supporting that standard could then ensure the safety of consumers' information by further encouraging compliance beyond PCI sanctions established by private contracts.[117]

The FTC has challenged entities that suffered data breaches by alleging that a "failure to maintain reasonable security is an unfair practice under the section 5 of the FTC Act."[118] The FTC has thus already taken a step in the direction of validating the PCI DSS as a national standard defining reasonable precautions that an entity should employ to protect consumer data and avoid potential liability. Congressional support of the same standard would produce predictable effects and support a familiar regime that can evolve over time in response to best practices in the industry.

C. Notification

Requiring notification following the exposure of personal financial information should not raise controversy. Because most states

---

113. *See* Thaw, *supra* note 57, at 321.

114. *See id.* at 321-23.

115. *See* MacCarthy, *supra* note 26, at 271 & n.65, 274.

116. *See* Thaw, *supra* note 57, at 293. Such deference to outside standards would not be unprecedented, as Congress referenced outside agencies to consult on evolving standards for the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, §§ 262(a), 264(d), 110 Stat. 1936, 2021, 2034 (1996) (codified in scattered sections of 42 U.S.C.), and the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 204, 508(b), 113 Stat. 1338, 1391, 1442-43 (1999) (codified in scattered sections of 12 and 15 U.S.C.), to ensure that experts, who are in the best position to understand the changing nature of data in the industry, can influence the security standard. *See* Thaw, *supra* note 57, at 313-15.

117. *See* Thaw, *supra* note 57, at 293.

118. MacCarthy, *supra* note 26, at 251. *See generally* Hutchins & Francois, *supra* note 50, at 48-50.

already enforce some type of notice requirement to lessen the effect of data breach harm, a federal standard would serve to unify expectations without changing the underlying policy already in place.[119]

State laws typically structure notification requirements by:

> (1) delineating who must comply with the law;
> (2) defining the terms "personal information" and "breach of security";
> (3) establishing the elements of harm that must occur, if any, for notice to be triggered;
> (4) adopting requirements for notice;
> (5) creating exemptions and safe harbors;
> (6) clarifying preemption and relationships to other federal laws; and
> (7) creating penalties, enforcement authorities, and remedies.[120]

Congress must first determine whether the requirement will apply to all entities or create exceptions for smaller businesses, nonprofits, or government entities. The provision should provide as few exceptions as possible to meet the purpose of preventing further harm resulting from a data breach. Even if smaller entities do not have the same resources as larger organizations in order to prevent breaches from occurring in the first place, small entities can still notify customers of a breach.

Congress would then need to define the type of information that, if exposed, would trigger notification duties. Describing such information as "personally identifiable information," states have protected "an individual's first name or initial and last name combined with S[ocial]S[ecurity]N[umber]; driver's license or state ID number; account number, credit or debit card number, combined with any required information that allows access to account or any other financial information."[121] Similarly, a federal standard should seek to protect any information not obtainable through public records that would connect an individual's identity to a sensitive piece of information, such as a Social Security Number or financial account data. This meets the overall goal of notifying customers when

119. *See supra* Part II.B.
120. STEVENS, *supra* note 56, at 5.
121. *Id.* at 6.

hackers have exposed potentially threatening information, thus allowing the individual and other affected entities to respond and minimize further loss.

Congress should exercise caution with regard to safe harbors. Locking in certain protocols that limit liability could encourage entities to maintain static data security policies designed to avoid liability rather than protect data.[122] The stagnating effect of data encryption safe harbors on data security innovation demonstrates the potential difficulties of creating exceptions based on compliance with concrete standards.[123] Instead, Congress should tie its notification requirement to general compliance with a federal data standard outlined in the statute. That standard could then account for changing technology and prevent complacent procedures.[124]

Lastly, providing an effective remedy will allow enforcement of the notification provision. Though separate penalties may apply for noncompliance with the overall data security standard, specific notification damages will serve the goal of lessening the harm of data breaches once they occur. Some state statutes include private rights of action to recover damages caused by a failure to report in a timely manner, whereas other states simply provide statutory damages based on the number of violations and the time delay before proper reporting and notification.[125] A federal provision should implement statutory damages per violation in order to prevent mass litigation over difficult-to-measure consequential damages. In many cases, statutory damages could exceed actual damages and would thus serve to encourage compliance while still benefitting harmed individuals who may struggle to demonstrate the injury necessary to secure compensation.[126]

---

122. *See supra* Part III.B.

123. *See* Thaw, *supra* note 57, at 321-22, 362-65.

124. *See supra* Part III.B.

125. *See, e.g.*, CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2014), *amended by* 2015 Cal. Legis. Serv. 522 (West); S.C. CODE ANN. §§ 1-11-490, 39-1-90 (2014); VA. CODE ANN. § 18.2-186.6 (2015); *see also* STEVENS, *supra* note 56, at 7.

126. *See supra* Part II.D.

IV. EVALUATING THE PERSONAL DATA PRIVACY AND SECURITY ACT OF 2014

The proposed Personal Data Privacy and Security Act of 2014 (PDPSA) provides an example of the type of legislation that Congress could enact in response to the increased number of mass data breaches.[127] The Senate has taken no substantial action on the bill since Senator Patrick Leahy introduced the bill in January 2014.[128] Similarly, the House of Representatives has not made progress on the companion bill that Representative Carol Shea-Porter introduced in February 2014.[129]

Despite the apparent failure of the bill to gain any traction in Congress, the PDPSA nonetheless offers a starting point for conceptualizing how the legislature could accomplish the recommended goals set forth in Part III: to (1) reduce the occurrence of data breaches by shifting liability to the breached party, (2) provide an evolving standard of reasonable data protection, and (3) minimize consequential harm by establishing uniform notification requirements.[130] Although the PDPSA would make progress on each goal, it neither advocates a wholesale reallocation of liability to the breached party nor provides a clear standard for data protection.

A. Purpose and Scope

In its congressional findings, the Senate acknowledged that hackers have increasingly targeted large databases of consumer information and that such breaches pose a "serious threat to the Nation's economic stability."[131] To address the threat, the PDPSA

127. Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong.

128. *All Bill Information (Except Text) for S.1897 - Personal Data Privacy and Security Act of 2014*, CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/senate-bill/1897/all-info [https://perma.cc/DBQ9-LAF4] (last visited Feb. 21, 2016).

129. *All Bill Information (Except Text) for H.R.3990 - Personal Data Privacy and Security Act of 2014*, CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/house-bill/3990/all-info [https://perma.cc/V6AG-JP5D] (last visited Feb. 21, 2016).

130. *See supra* Part III.

131. S. 1897 § 2(2). President Obama expressed a similar concern, issuing an Executive Order in February 2013 designed to improve cybersecurity. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 19, 2013) ("The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.");

suggests that business entities should "adopt reasonable procedures to ensure the security, privacy, and confidentiality of ... personally identifiable information."[132] The recommendation comports with this Note's assertion that merchants should be held liable for harm resulting from data breaches, and that the burden should not rest primarily with issuing banks.

The PDPSA applies to "[a] business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons."[133] Limiting the applicability to businesses that maintain the data of a significant number of consumers prevents small businesses from falling under the burden of extensive data protection requirements. Yet, many small businesses still may fall within the PDPSA given the common exchange of personal information.

The extensive types of protected data reveal more about the scope of the PDPSA than the quantity threshold. Under the PDPSA's definition, "sensitive personally identifiable information" includes any of the following combinations of information: (1) first initial, last name, phone number, and date of birth; (2) driver's license number; or (3) financial account number.[134] The same information could be located on a Facebook account, displayed while making an alcohol purchase, or disclosed by using a check or credit card. The real threat is not the information itself, but the accumulation of thousands of records in one location. The wide scope of protected data follows similar definitions used by states in their notification statutes, showing a widespread recognition that even basic information should receive protection.[135]

---

see also Press Release, The White House, Office of the Press Sec'y, Executive Order—Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [https://perma.cc/ H8DG-XB52].

132. S. 1897 § 2(4).

133. *Id.* § 201(b).

134. *Id.* § 3(11).

135. *See supra* note 56 and accompanying text.

B. Prevention Through Allocation of Liability

The PDPSA addresses the first goal—to encourage private entities to employ stronger preventative measures and avoid future data breaches—by (1) imposing civil penalties for failure to meet a level of reasonable data protection and (2) allowing equitable relief to enjoin private entities from operating in violation of data security standards.[136] The PDPSA would not force a wholesale reallocation of liability from issuing banks to merchants; instead, the enforcement measures seek to reduce the overall occurrence of breaches by incentivizing businesses to take greater precautions and avoid statutory liability.[137]

The PDPSA empowers the FTC to enforce the proposed data protection requirements.[138] Granting clear authority to the FTC makes sense given the FTC's current efforts to enforce data security under section 5 of the FTC Act.[139] The PDPSA would expand the FTC's authority and provide a more solid ground to impose sanctions on entities that fail to meet a reasonable standard of protection.

1. Civil Penalties

Either the FTC or a state enforcement agency may seek civil penalties of up to $1 million if a business fails to follow data protection requirements.[140] The enforcement scheme initially assesses up to $5000 per violation per day that the violation continues.[141] Typically, the total sum resulting from one act or omission would not exceed $500,000.[142] If the court determines that the act or omission constituted willful or intentional conduct, the court could

136. *See* S. 1897 §§ 102, 203.

137. *See id.*

138. *Id.* § 203(b). Apart from the FTC, state enforcement agencies may also bring a claim against business entities in district court if violations under the statute harm residents of the state. *Id.* § 203(c). The State could seek civil penalties or equitable relief to enforce compliance. *Id.*

139. *See supra* Part II.A.

140. S. 1897 § 203(a)-(c)(2).

141. *Id.* § 203(a)(1), (c)(1)(C).

142. *Id.*

impose additional penalties of $5000 per willful or intentional violation per day, also capped at $500,000.[143]

When measured against the substantial harm caused by data breaches and the potential liability shared between merchants and banks, the civil penalties outlined in the PDPSA offer virtually no additional incentive to implement a data security program. In the Target data breach alone, Target spent $61 million in one quarter and faced over eighty lawsuits.[144] Experts estimated that the breach will result in $1.4 billion to $2.2 billion in fraudulent charges made using stolen financial information.[145] Target could also face fines between $400 million and $1.1 billion from the PCI Council.[146] Given that the potential harm caused by violating the data protection requirements could range in the billions, civil penalties capped at $1 million (and even then only for willful or intentional acts or omissions) hardly seem adequate to influence behavior.

The liability assignment would be more powerful if the penalty or damages applied to each individual record that the entity failed to protect, rather than the overall violation. The Fair Credit Reporting Act (FCRA), for example, imposes statutory damages between $100 and $1000 for each instance.[147] Under that model, the liability that the party failing to protect consumer information incurred would vary based on the number of people harmed, not just the number of security violations.[148]

If Congress calculated liability based on the number of data records involved, then it would have to determine a reasonable dollar limit per record. At the FCRA maximum of $1000 per person, a merchant, such as Target, would be liable for $110 billion based on the 110 million records exposed—clearly an excessive amount. Since the customers themselves face minimal actual damages, a reasonable figure should derive from the harm the breach causes the issuing banks, who bear the brunt of the damages.[149] Though the

143. *Id.* § 203(a)(2)-(3), (c)(2).

144. TARGET CORP., FORM 10-K, ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGE ACT 16-17 (2014), http://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm [https://perma.cc/U9CY-A88R].

145. WEISS & MILLER, *supra* note 5, at 6.

146. *Id.*

147. Fair Credit Reporting Act of 1970 § 616, 15 U.S.C. § 1681n(a)(1)(A) (2012).

148. *Id.*

149. *See supra* Part I.C.2.

actual costs incurred as a result of data breach vary among banks, a figure of $10 per consumer would cover most, if not all, consequential harm.[150] Under a cap of $10 per violated customer, Target would be liable for up to $1.1 billion due to its data breach. Of course, a court could decide to award any fraction of the maximum figure. Assessing damages based on the number of violated customers and the costs associated with the breach would force merchants to internalize the costs associated with data breaches and take adequate precautions to avoid liability.

Congress would also need to decide to whom payments would be disbursed. Civil penalties do not compensate parties that suffer damages as a result of the breach; they pose an incentive only to maintain proper data security. The minimal deterrent effect of civil penalties would mean little to banks faced with actual breach-related damages. Instead of treating the $1.1 billion liability ($10 per record) as a civil penalty, Congress should allow courts to disburse awards, not to exceed the cap, to parties harmed by the breach. One district court would consolidate all claims against the breached party, assess damages, and accordingly award the litigants damages. In the event that the actual damages fall short of the cap, the remainder could be collected as a penalty if the judge decided to do so.

The recommended amendment to the civil penalties provision would force businesses to consider the full cost of a potential breach and provide an opportunity to compensate injured parties for the breached party's failure to take reasonable precautions. Of course, some data breaches will occur even with data security protocols, and in those situations the breached party would not be liable under the statute if it exercised due care.

Neither the PDPSA nor the recommended damages scheme would affect the ability of private parties to further allocate liability by contract. Legislation would simply set the logical baseline that a party who fails to exercise due care should be liable for the harm that ensues.

150. *See supra* notes 43-44 and accompanying text.

2. Equitable Relief

In addition to the civil penalties discussed above, the PDPSA also permits courts to enjoin a business from allowing a violation to continue.[151] The court's equitable power reduces the concern that a business may intentionally fall below the industry standard because it deems noncompliance more economically efficient.

A business would be unlikely to face an injunction until there has already been a breach of security, as the FTC will not be in a position to investigate compliance for every entity. So, while an injunction may prevent further harm, it would not serve as a strong incentive to avoid violations up front. Given the reactionary nature of the injunctive relief, this provision does little to incentivize robust data security precautions. Nonetheless, it would provide a safety net to prevent companies from continuous, willful violation of the statute.

C. Evolving Standards Based on the PCI DSS

An important part of prevention depends on setting an appropriate standard that can evolve over time with industry standards and with changes in technology. For the purposes of the federal statute, Congress must decide who should set the standard and what that standard should entail.

1. Who Sets the Standard?

The PDPSA involves several parties in the development of a data protection standard. Rather than creating a definite standard itself, the PDPSA seeks to "*ensure* standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personally identifiable information."[152] Businesses must maintain "protection equal to industry standards or standards widely accepted as an effective industry practice."[153] The PDPSA empowers the FTC to determine the

151. Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. § 203(a)(4).
152. *Id.* § 201(a) (emphasis added).
153. *Id.* § 201(d).

appropriate industry standard on a case-by-case basis, depending on the type of information involved and the characteristics of the business.[154]

In reality, this probably means that the PCI DSS would set the bar for reasonableness in the credit card payment industry for two reasons. First, since credit card companies and payment processors already use and require compliance with the PCI DSS, the protocols set by the PCI are, in fact, the industry standard.[155] The PDPSA would require businesses that have not contracted with a PCI member to still comply with that standard because it represents custom in the industry. Second, the FTC currently looks to the PCI DSS for a reasonable standard of data security when investigating its claims of unfair practices under section 5 of the FTC Act.[156] There is no apparent reason why the FTC would abandon its understanding of the industry norm in favor of a new standard.

Despite the FTC's role as the interpreter of the reasonable industry standard and the PCI DSS's likely guidance in defining the standard, the PDPSA provides a large degree of flexibility that allows each entity to implement a viable and effective plan. In fact, under the bill, the lack of a specific practice or technology cannot alone result in noncompliance. Enforcers first must consider the entity's data plan as a whole.[157] This allows private entities to develop cost-effective programs best suited to protecting their information. Specifically, it prevents the creation of a static safe harbor that marks illusory compliance rather than encourages actual security. The next Section discusses the boundaries set by the statute within which each company can develop its own data privacy and security program.

2. Statutory Requirements

The PDPSA requires each qualifying entity to implement a comprehensive personal data privacy and security program.[158] Programs include administrative, technical, and physical safeguards that vary

154. *Id.*
155. *See supra* Part II.C.
156. *See supra* Part II.A.
157. S. 1897 § 201(d).
158. *Id.* § 202(a).

depending on the size of the business and the type of information stored.[159] In order to allow this variance, the PDPSA provides broad guidelines on developing a comprehensive plan, but does not require any specific measure.[160]

First, the program must be designed with the following goals: to (1) ensure the security of personal information, (2) protect against "anticipated vulnerabilities," and (3) "protect against unauthorized access to ... information."[161] If accomplished, meeting these goals would reduce data breaches significantly. Of course, some breaches would come from unanticipated vulnerabilities and, despite adequate measures, the program may not always operate effectively.

Second, the program must include a risk assessment in which the business shall: (1) "identify reasonably foreseeable internal and external vulnerabilities;" (2) "assess the likelihood of and potential damage from unauthorized access;" (3) "assess the sufficiency of its policies, technologies and safeguards in place to control and minimize risks from unauthorized access;" and (4) "assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information."[162] This phase of the plan requires businesses to gather the information necessary to protect their data. Rather than create a uniform set of procedures, the PDPSA guides companies though a self-diagnosis to determine where data protection measures will effectively reduce the potential risk of harm to individuals who trusted their data to the company.[163]

Identifying internal and external vulnerabilities shows potential points of entry where the business needs to place protective barriers to keep hackers and unauthorized users away from sensitive information. Calculating the likelihood and potential damage from unauthorized access helps entities allocate resources efficiently by placing the most extensive security in areas where the risk of harm poses the greatest threat. Assessing the sufficiency of current policies and technologies recognizes the gap between present data protections and the desired security identified above. Lastly, assessing the vulnerability of information during destruction or disposal

159. *Id.*
160. *See id.*
161. *Id.* § 202(a)(2).
162. *Id.* § 202(a)(3).
163. *Id.*

reminds entities to protect sensitive data even when it no longer serves an internal purpose.

Third, the company must institute reasonable measures to manage and control the risk. In this stage, the business must take precautions appropriate for the size of the entity, the sensitivity of its data, and the nature of its activity.[164] These security measures must: (1) control access to systems and facilities containing sensitive information; (2) detect and record information about actual and attempted unauthorized access to sensitive material; (3) protect sensitive data by using encryption or access controls common in the industry; (4) ensure proper destruction of sensitive information; (5) trace credentials of users who have gained access to information; and (6) prevent third parties from accessing information without first passing a company review.[165] Additionally, the plan should limit the amount of personally sensitive data retained.[166]

The elements of the comprehensive personal data privacy and security program leave significant discretion to individual entities. Each of the requirements above ensures that the entity asks the proper questions when developing a plan to protect sensitive information. More importantly, the PDPSA does not limit the applicability of the standard to one place and time.[167] Instead, the guidelines set forth can evolve over time, and programs can change with new technology, as they must. These risk control factors find a proper balance between a clear statutory framework and a flexible standard that can evolve over time.

D. Notification

The PDPSA requires that entities provide customers with notice regarding data breaches within a reasonable period of time.[168] The PDPSA would allow an entity to delay notice only for the time necessary to determine the scope of the security breach, assess the risk posed to its customers, and restore the integrity of its data

164. *Id.* § 202(a)(4)(B).
165. *Id.*
166. *Id.* § 202(a)(4)(C).
167. *See id.* § 201(d)(1).
168. *Id.* § 211(a)-(c).

system.[169] This investigation, conducted prior to notification, generally would not exceed sixty days, but the breached party could obtain an extension from the FTC if necessary.[170]

The initial sixty-day limit strikes a balance between the entity's need to evaluate the extent of the breach and the customer's desire to avoid future harm. By limiting the time frame, the PDPSA ensures that businesses will not intentionally drag their feet following a breach to avoid disclosure. Without an investigatory period, the breached party would not actually be able to provide much useful information to its customers because it would not yet know the extent of the breach or the risk posed. The delay also allows enough time to strengthen security protocols, rather than inviting more attacks while still vulnerable.

There are two significant exceptions to the notification requirement. First, the Secret Service or the FBI may decide to restrict notification in the interests of national security.[171] The second, and more relevant to this Note, releases businesses from notification responsibilities if "there is no significant risk that a security breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm to the individuals whose sensitive personally identifiable information was subject to the security breach."[172] The business makes this determination after performing a required risk assessment and must provide notice to the FTC of its intent to invoke the exception within forty-five days.[173] The FTC then has ten days to respond with a contrary determination that the business must provide notification.[174] If no substantial risk of harm exists, then the company does not have to expend extensive resources providing notice, answering consumer concerns, and repairing its damaged brand.[175]

Whether the breach poses a risk of substantial injury depends on the type of data stolen and the condition in which the hacker obtained the information. The PDPSA follows state law models that

169. *Id.* § 211(c).
170. *Id.*
171. *Id.* §§ 211(d), 212(a).
172. *Id.* § 212(b).
173. *Id.*
174. *Id.*
175. *See supra* Part I.C.

create an exemption by establishing a limited safe harbor for businesses using encrypted data.[176] Rather than creating a blanket safe harbor, the PDPSA establishes only a rebuttable presumption that the encryption of personally identifiable information presents no significant risk.[177] Similarly, any method of making the information "unusable, unreadable, or indecipherable through data security technology" would also create a rebuttable presumption that the breach does not pose a significant risk.[178]

The rebuttable presumption avoids the dangerous incentive of a safe harbor that encourages compliance with just one aspect of a data protection plan. At the same time, the presumption rewards entities for taking measures to protect stored data. Generally, the presumption should prove true and notice would not be required, but the FTC oversight protects consumers if, in a particular breach, encryption alone does not mitigate the threat of further harm.

The notification provisions set forth by the PDPSA do not create any surprising requirements. Rather, the regulations mirror the most common state law statutes.[179] The importance of a federal notification provision rests in the uniform standard established nationwide. Instead of interpreting many different state laws, businesses would have only to follow one notification scheme, making notification easier and clearer for businesses.

As previously noted, the state notification statutes do not prevent data breaches from occurring, nor do they shift any liability from the issuing banks to the merchant.[180] Notification simply requires businesses to disclose information regarding the breach and to alert customers to potential harm following the release of personal information.[181] Nonetheless, the reduction in consequential damages certainly makes the notification requirement valuable, particularly in conjunction with a uniform standard.

176. *See supra* note 60 and accompanying text.
177. *See* S. 1897 § 212(b)(2).
178. *Id.*
179. *See id.* § 211; *see also supra* notes 56-59 and accompanying text.
180. *See supra* Part II.B.
181. *See supra* Part II.B.

E. Overall Assessment

The PDPSA takes a significant step toward protecting consumers from data breaches. Merchants, such as Target, would have to create a comprehensive data security program to prevent data breaches from occurring, pay fines for failure to prevent breaches through reasonable precautions, and notify customers when they face a risk of harm from the breach.[182]

The data standard itself meets the suggestion for a data security standard based on the PCI DSS. Although the PDPSA does not explicitly identify the PCI, it calls for an industry standard interpreted by the FTC.[183] Importantly, the PDPSA does not simply adopt the PCI standard, but enables its use by establishing a broad framework of considerations under which companies must create their own data programs. Entities would be well-advised to base their programs on recommendations made by the PCI, but the statute would allow that standard to change over time in response to new technology and new threats.

The civil penalties imposed by the PDPSA would have little effect. The potential penalties pale in comparison to the substantial losses that the parties would collectively suffer.[184] Given the costs paid by merchants alone, the penalties do not create much of an incentive to comply. Further, the penalties do not seek to compensate those harmed the most—issuing banks—and do not attempt to reallocate the liability caused by a breach. The PDPSA's failure to meet this goal probably derives from its focus on protecting consumers rather than issuing banks. Nonetheless, ignoring this problem prevents merchants from fully internalizing the cost of noncompliance with security standards.

Lastly, the PDPSA notification requirement addresses the problem of inconsistent state statutes. The consumer notice obligation offers reasonable time frames and exemptions to protect businesses from unnecessary costs following a breach with a low risk of harm.

---

182. In the Target example, a properly executed program would have prevented the third-party vendor from having access to the sensitive information that hackers eventually stole. *See supra* Part I.A.

183. S. 1897 § 202(a).

184. *See supra* Part IV.B.1.

At the same time, it reduces consequential damages by enforcing notice when the breach poses a substantial risk to consumers.

On the whole, the PDPSA would improve the current state of data protection. However, the failure to address the imbalance between merchants and issuing banks leaves the door open for future data breaches based on inadequate incentives to provide stronger data security protections.

V. COUNTERARGUMENTS

Creating and enforcing a federal standard will no doubt face much criticism. The following counterarguments raise and refute theoretical concerns in opposition to a congressional approach.

A. Private Entities Should Be Able to Allocate Risk by Contract

One theoretical argument in opposition is that private entities are in the best position to understand the risk associated with their private business transactions. Since the parties themselves can allocate risk by contract, Congress does not need to pass any legislation that would frustrate the market.

This argument fails to recognize that the problems with the current system stem from the lack of uniform guidelines. The volume and scope of data breaches themselves show that private entities in the market cannot successfully protect user data. When a breach occurs, the effects ripple throughout the payment card industry, from the customer to the merchant and the issuing bank, among others.[185] Suggesting that each of these parties should enter into contractual agreements with one another stretches the realm of possibility. The transaction costs necessary to effectuate the volume of agreements sufficient to cover the entire industry would be cost-prohibitive.[186]

Although two parties—such as the merchant and the customer, the issuing bank and the payment processing company, or the merchant and the acquiring bank—may be able to negotiate an acceptable agreement, some entities that bear risk cannot enter into

185. *See supra* Part I.C.

186. *See generally* Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

contractual relationships with those that control that risk.[187] At best, these companies can argue that they constitute third-party beneficiaries of existing contracts. However, courts have been reluctant to accept that argument to find liability.[188]

The creation of a congressional structure that allocates risk to the merchant when the merchant fails to meet a reasonable standard of care would not prevent parties from continuing to contract around liability. Merchants could still pass on their liability by contract to banks or insurance providers, but they would simply have to pay to pass on the risk (that the merchant can control) to a third party.

B. Congress Does Not Need to Implement Protection for Sophisticated Parties

In an argument similar to the one outlined above, opponents could argue that sophisticated parties do not need congressional assistance to allocate risk or set data security standards. This assertion ignores the varying size of entities harmed by data breaches and attacked by hackers. In fact, smaller banks suffer at a much higher rate than larger banks in the wake of data security breaches.[189] While large banks may be capable of negotiating contracts to shift liability, the small banks would likely struggle to do so.

A variation of the same issue arises among parties that store sensitive personal information. Large entities may be more capable of implementing data security precautions, whereas small companies may not have the same resources to spend on protection. The congressional approach would shift liability to protect less powerful banks and enforce standards tailored to the size of entities storing information.[190]

A set of uniform requirements protects all parties involved in payment transactions. Sophisticated parties have failed to allocate liability sufficient to reduce the occurrence of data breaches and to protect customers and issuing banks that do not have contractual

187. For example, the issuing banks cannot enter directly into agreements with every merchant, so they cannot privately agree on how they will share the risk of liability in the event of a data breach.

188. *See supra* Part II.D.2.

189. *See supra* Part I.C.2.

190. *See supra* Part IV.C.2.

relationships with merchants. The congressional approach instead provides all parties with a plan designed to protect against breach and allocate the risk accordingly, regardless of sophistication.

C. Reliance on the PCI DSS and Industry Standard Negates a Congressional Approach

If Congress implemented a uniform set of data security rules based on the PCI DSS, critics could argue that reliance on the PCI DSS or an "industry standard" means that Congress has essentially delegated its responsibilities back to private parties.

Under the PDPSA, there probably would not be a significant change in the requirements for data security.[191] The strength of the congressional approach is not that Congress will implement a revolutionary new standard, but that Congress will enforce the standard set by the industry and hold liable those responsible for a breach if they fail to take reasonable preventative measures. However, Congress would not blindly enforce a private standard. The PDPSA proposes that the FTC designate the standards by which it will evaluate the appropriateness of data security protocols.[192] At the moment, this would likely mean enforcement of the PCI DSS, but the FTC could add additional requirements or rely on a new standard as the industry changes.[193] The congressional approach looks to private industry to determine reasonableness, but ultimately the FTC and the federal courts would enforce compliance.

---

191. *See supra* Part IV.C.

192. *See supra* Part IV.C.

193. If Congress became concerned that the PCI standard presented a biased standard designed to shift undue liability to merchants by setting a high bar for security, then the FTC could create a committee for evaluating the industry and setting a standard. The committee could include a variety of interested parties, such as issuing banks, acquiring banks, card processing companies, and merchants. The variety of backgrounds and diversity of opinions would help create a reasonable data standard that fairly allocates risk among the parties.

CONCLUSION

The prevalence of electronic payment transactions, the widespread transmission of information, and the common storage of personal data have created an attractive target for hackers seeking to steal financial data for fraudulent purposes. Recent data breaches at large retailers demonstrate the significance of data privacy and security.

Despite this importance, private entities have failed to create adequate incentives to prevent data breaches. Merchants, a group that has suffered from many of the most recent high-profile attacks, bear a disproportionately low amount of the liability given their unique position to prevent data breaches from occurring. These data breaches incur huge costs totaling in the billions of dollars. Under the current system, the risk of liability generally rests with each harmed party, and not necessarily the merchant whose failed security measures allowed the breach.

This Note argues that Congress should pass legislation to hold companies liable for data breaches if they fail to exercise due care in protecting the information. To date, harmed parties, particularly issuing banks, have been unsuccessful at recovering damages from the breached party through existing legal standards.[194] Successful legislation should aim to: (1) encourage the prevention of data breaches by allocating liability to the breached party, (2) evolve with industry standards to avoid outdated and ineffective requirements, and (3) require uniform notification guidelines following a data breach.

The Personal Data Privacy and Security Act of 2014 presented a viable option for congressional enforcement of the data privacy and security standards in the payment card industry. While the PDPSA would meet the goals of providing uniform notification guidelines and evolving with industry standards, it would fail to adequately incentivize merchants to implement changes or compensate harmed parties. Amendments to secure these important objectives would make legislation like the PDPSA a strong measure

194. *See supra* Part II.D.

to promote data security and protect all parties involved in electronic payments.

Justin C. Pierce[*]

* J.D. Candidate 2016, William & Mary Law School; B.A. 2013, with Distinction, University of Virginia. I would like to thank my family and friends for their constant support throughout Law School and beyond, especially Cindi Steele, Cliff Pierce, Brandon Pierce, and Monica Dominguez. My ability—hopefully—to write clear and coherent arguments owes great gratitude to John Wilkes, Joseph Miller, and Charles McCurdy, each of whom sacrificed many hours coaching me through previous written works. Lastly, many thanks to the *William & Mary Law Review* editors and staff for their hard work in preparing this Note for publication. For student editors, the cite-checking and revision process can be overwhelming, if not miserable at times. With particular attention to this burden, I offer my appreciation for every bit of energy placed in this Note.