Incentivizing the Protection of Personally Identifying Consumer Data After the Home Depot Breach

RYAN F. MANION*

INTRODUCTION

Identity theft in the United States is commonly viewed as a growing problem.[1] However, the best available data indicates that certain types of identity theft are growing while other forms are becoming less common.[2] The most discernible problem for individuals worried about identity theft remains the disclosure of sensitive personal data, such as social security numbers. Examples of recent data breaches at major companies—Target,[3] Sony,[4]

---

* J.D. Candidate, 2016, Indiana University Maurer School of Law; B.A., 2008, University of Richmond. I would like to thank all of the members of the *Indiana Law Journal* that helped prepare this Note for publication. Further, I would like to thank my family and close friends, who undoubtedly have endured more conversations about data breaches than they ever thought possible.

1. *See, e.g.*, Sloane v. Equifax Info. Servs., LLC, 510 F.3d 495, 505 (4th Cir. 2007) ("[I]dentity theft has emerged over the last decade as one of the fastest growing white-collar crimes in the United States."); Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) (finding an "alarming increase in identity theft in recent years").

2. There was a total of 290,056 identity theft complaints reported to the Federal Trade Commission's Consumer Sentinel Network (CSN) in calendar year 2013, which represented 14% of over 2 million complaints received (excluding do-not-call). FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY–DECEMBER 2013 3, 5 (2014). There were 246,035 identity theft complaints to CSN in calendar year 2006, which represented 36% of over 670,000 total complaints. FED. TRADE COMM'N, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA JANUARY–DECEMBER 2006 3, 5 (2007). The Department of Justice also keeps statistics on identity theft. Roughly 7% of persons age sixteen or older were victims of identity theft in 2012. ERIKA HARRELL & LYNN LANGTON, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012, at 1 (2013). Eighty-five percent of all identity theft incidents involved the use of an existing account. *Id.* at 1–2. Meanwhile, the Department of Justice's 2008 report indicates that about 5% of all persons age sixteen or older dealt with identity theft, but only 53% of the theft was attempted unauthorized use of existing credit cards, although that percentage might be higher if other account information, such as bank account numbers, were added. LYNN LANGTON & MICHAEL PLANTY, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2008, at 1 (2010). New account fraud numbers are nearly identical between the 2008 and 2012 reports, with less than 1% of victims reporting this issue in both years. *Id.*; HARRELL & LANGTON at 2. The number of existing account incidents grew from 8,339,500 in 2008 to 15,323,500 in 2012. LANGTON & PLANTY at 2; HARRELL & LANGTON at 2. Thus, it seems that existing account fraud or identity theft is growing, while new account fraud is remaining stable.

3. Brian Krebs, *Sources: Target Investigating Data Breach*, KREBSONSECURITY (Dec. 19, 2013, 8:20 AM), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ [http://perma.cc/T9MF-9EDC].

4. Jeff Stone, *Sony Hacked: PSN Safe, but Computer System Offline After Malicious Threat: Report*, INT'L BUS. TIMES (Nov. 25, 2014, 9:54 AM), http://www.ibtimes.com/sony-hacked-psn-safe-computer-system-offline-after-malicious-threat-report-1729073 [http://perma.cc/7B3C-98QC].

JPMorgan Chase,[5] and the Home Depot,[6] to name a few—demonstrate that disclosure of personal information to unauthorized third parties must be prevented to ensure security.[7]

The breach of payment card systems at the Home Depot in 2014 resulted in the theft of a wealth of information.[8] This Note will examine the facts and legal consequences of the Home Depot breach under three separate frameworks. First, this Note will examine the Home Depot's responsibilities arising under existing data breach notification statutes. Second, this Note examines the Home Depot's potential liability if the recent bill introduced by Senator Leahy of Vermont proposing a federal data breach notification framework becomes law;[9] ultimately, however, this Note finds that state notification statutes fail to adequately protect consumers, and Senator Leahy's bill, while better suited than existing state notification statutes, is unlikely to be effective. Lastly, this Note examines the Home Depot's potential liability if the Federal Trade Commission (FTC) were to adopt a penalty structure similar to those in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and concludes that a data protection model that imposes similar kinds of penalties for companies that suffer breaches of sensitive consumer data would better serve the public interest.[10]

---

5. Supriva Kurane, *JPMorgan Data Breach Entry Point Identified: NYT*, REUTERS (Dec. 22, 2014, 10:09 PM), http://www.reuters.com/article/2014/12/23/us-jpmorgan-cybersecurity-idUSKBN0K105R20141223 [http://perma.cc/Y29D-CH43].

6. Brian Krebs, *Banks: Credit Card Breach at Home Depot*, KREBSONSECURITY (Sept. 2, 2014, 1:50 PM), http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/ [http://perma.cc/HLA2-PAT9].

7. *See, e.g.*, Team BillGuard, *Home Depot Data Breach Likely to Strike 60 Million and Cause Over $2 Billion in Fraud*, FOLLOW THE MONEY BY BILLGUARD (Sept. 18, 2014), http://blog.billguard.com/2014/09/home-depot-data-breach-estimated-impact/ [http://perma.cc/29FJ-HFJ3].

8. Approximately fifty-six million cards and fifty-three million e-mail addresses were breached. Press Release, The Home Depot, The Home Depot Reports Findings in Payment Data Breach Investigation (Nov. 6, 2014); *Home Depot: Data Breach Hits 56M Cards*, ALJAZEERA AM. (Sept. 18, 2014, 8:01 PM), http://america.aljazeera.com/articles/2014/9/18/home-depot-data-breach.html [http://perma.cc/288F-32JF].

9. Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015). An identical bill exists in the House of Representatives. Consumer Privacy Protection Act of 2015, H.R. 2977, 114th Cong. (2015).

10. Similar, but not exactly the same, solutions have been proposed by other authors. *See* Rachel Yoo, *An Expected Harm Approach to Compensating Consumers for Unauthorized Information Disclosures*, 19 RICH. J.L. & TECH. 1, 50–52 (2012) (proposing a penalty scheme based off of HITECH but before the most recent Department of Health and Human Services Amendments were implemented). In addition, others have articulated the need for an omnibus data breach law. *See, e.g.*, Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517 (2010); Jill Joerling, Note, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467 (2010). Such a law is necessary, but this Note focuses on the penalty scheme that should be included in a federal data protection law.

I. THE HOME DEPOT BREACH OF 2014

A. The Facts Associated with the Breach

In September 2014, a number of banks identified the Home Depot as the source of a massive data breach of consumer credit and debit card information.[11] Within days it was revealed that approximately fifty-six million credit and debit cards, along with about fifty-three million e-mail addresses, had been compromised in a breach of the Home Depot's self-checkout computer systems.[12] At the time, it was the second-largest breach of consumer data in history, far surpassing the Target breach of 2013.[13] The damage was extensive. Community banks reissued approximately 7.5 million new credit and debit cards and absorbed nearly $90 million in costs.[14] The expected amount of fraudulent charges as a result of the breach was as high as $3 billion, with an average fraudulent purchase of $332 per compromised card.[15]

The Home Depot responded quickly to the breach of its payment systems. The breach was fixed within days, and the Home Depot implemented enhanced encryption of payment data.[16] The implementation of chip-and-PIN security technology, a more secure way of processing credit and debit card transactions,[17] and enhanced encryption techniques were fast-tracked in the Home Depot's U.S. stores (chip-and-PIN technology has been in the Home Depot's Canadian stores since 2011).[18] The Home Depot offered free identity theft protection through AllClear ID for one year to every person who had made a purchase at an affected Home Depot store during the breach.[19]

---

11. *See* Krebs, *supra* note 6.

12. The Home Depot, *supra* note 8; Nicole Perlroth, *Home Depot Says Data from 56 Million Cards Was Taken in Breach*, N.Y. TIMES: BITS (Sept. 18, 2014, 8:21 PM), http://bits.blogs.nytimes.com/2014/09/18/home-depot-says-data-from-56-million-cards-taken-in-breach/?_php=true&_type=blogs&_r=2 [http://perma.cc/4DKD-47PN].

13. Target's breach was approximately 40 million cards, but others believe it to be worse for other reasons. *See, e.g.*, Catey Hill, *Home Depot's Data Breach is Worse than Target's, so Where's the Outrage?*, MARKETWATCH (Sept. 25, 2014, 11:28 AM), http://www.marketwatch.com/story/yawn-who-cares-about-home-depots-data-breach-2014-09-24 [http://perma.cc/VBB3-2Q9D].

14. Phil W. Hudson, *Home Depot Data Breach Cost Community Banks $90M, Report Says*, ALB. BUS. REV. (Dec. 21, 2014, 9:20 PM), http://www.bizjournals.com/albany/news/2014/12/21/home-depot-data-breach-cost-community-banks-90m.html [http://perma.cc/YYR4-QXRA].

15. Team BillGuard, *supra* note 7; *see also* Reuters, *Data Breach at Home Depot Leads to Fraud*, FORTUNE (Sept. 23, 2014, 7:35 PM), http://fortune.com/2014/09/23/data-breach-at-home-depot-leads-to-fraud/ [http://perma.cc/8796-224V] (describing how criminals were using the stolen credit card information).

16. The Home Depot, *supra* note 8.

17. Becky Krystal, *The Basics of Chip-and-PIN Credit Cards*, WASH. POST (May 16, 2013), http://www.washingtonpost.com/lifestyle/travel/the-basics-of-chip-and-pin-credit-cards/2013/05/16/9e8bdf9a-a13f-11e2-be47-b44febada3a8_story.html [http://perma.cc/K7VJ-5QUF] (explaining the basics of chip-and-PIN technology).

18. The Home Depot, *supra* note 8.

19. Press Release, The Home Depot, FAQs: November 6th Email Announcement (Nov.

B. Legal Fallout of the Breach

The Home Depot reportedly was not vigilant in maintaining the security of its systems before the breach was discovered.[20] As a result, customers have filed a plethora of lawsuits in numerous jurisdictions,[21] despite the recognition by the Home Depot that it (or the card-issuing financial institution) is responsible for related fraudulent charges on the compromised payment cards.[22] In the wake of the breach, major class action lawsuits were filed on behalf of consumers in Georgia and California.[23] Those consumer suits were combined with a class action suit on behalf of affected banks, and now the combined class action suit is pending in Georgia.[24]

II. POSSIBLE FORMS OF CONSUMER PROTECTION

Currently, consumers are protected mostly under state law in the event of a breach. Some states, however, are considering altering the scope of their laws, and Congress is considering a federal data breach notification law. Additionally, the FTC has the power to prevent the use of deceptive trade practices. This Part will explore the existing sources of consumer protection by examining three state laws that are indicative of the different approaches adopted by the states, a current proposal from Senator Leahy in Congress to enact a federal data breach notification law, and the effectiveness of HIPAA and HITECH regulations on the health care industry.

6, 2014), *available at* https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf [https://perma.cc/Q4U6-95BP].

20. *E.g.*, Julie Creswell & Nicole Perlroth, *Ex-Employees Say Home Depot Left Data Vulnerable*, N.Y. TIMES, Sept. 19, 2014, http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html [http://perma.cc/43E6-H3FT]. The Home Depot also claimed that "the malware used in the attack had not been seen in any prior attacks." The Home Depot, *supra* note 8. The Home Depot's claim may not be entirely accurate given reports that the malware was a new variant of the malware that infected Target's systems months beforehand. Brian Krebs, *Home Depot Hit by Same Malware as Target*, KREBSONSECURITY (Sept. 7, 2014), http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/ [http://perma.cc/2RN6-P93A].

21. *See* Kevin McGinty, *Home Depot Data Breach Litigation: Venue and Consolidation*, MINTZ LEVIN (Nov. 5, 2014), http://www.privacyandsecuritymatters.com/2014/11/home-depot-data-breach-litigation-venue-and-consolidation/ [http://perma.cc/Y9YC-2345].

22. The Home Depot, *supra* note 19.

23. Earls v. The Home Depot Inc., No. 3:14-cv-4315, (N.D. Cal. filed Sept. 24, 2014), *consolidated into In re* Home Depot, Inc. Customer Security Breach Litigation, No. 1:14-md-02583 (N.D. Ga.), *available at* http://www.girardgibbs.com/blog/wp-content/uploads/Home-Depot-Data-Breach-Class-Action-Complaint.pdf [http://perma.cc/G3XF-GW3N] (original California complaint); Solak v. The Home Depot, No. 1:14-cv-02856-WSD, (N.D. Ga. filed Sept. 4, 2014), *consolidated into In re* Home Depot, Inc. Customer Security Breach Litigation, No. 1:14-md-02583 (N.D. Ga.).

24. *In re* Home Depot, Inc. Customer Security Breach Litigation, No. 1:14-md-02583 (N.D. Ga. filed Dec. 11, 2014).

A. State Data Breach Notification Laws

States have attempted to protect their residents from identity theft by ensuring that swift, remedial action is available to consumers.[25] Forty-seven states and the District of Columbia have passed data breach notification laws requiring notification to consumers whose personally identifiable information is compromised in a security breach.[26] Typically, these statutes contain similar provisions, including the entities that must comply, a definition of "personal information," a definition of "breach," the requirements of notice, and any exemptions.[27] The following subparts will examine the breach notification statutes of Georgia and California, where class action lawsuits against the Home Depot were originally filed, and Indiana to demonstrate the common provisions of these laws.

1. Georgia

Georgia's Security Breach of Computerized Personal Information Act requires,

> Any information broker or data collector that maintains computerized data that includes personal information of individuals [to] give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[28]

A "data collector" is limited to a "state or local agency or subdivision thereof,"[29] and an "information broker" is an "entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties."[30] Personal information is defined as an individual's first name or initial and last name combined with: (1) the individual's social security number; (2) driver's license or state identification number; (3) an account, credit

---

25. *See, e.g.*, GA. CODE ANN. § 10-1-910(1) (2009) ("The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sectors."); *Id.* § 10-1-910(3) ("Identity theft is one of the fastest growing crimes committed in this state."); *Id.* § 10-1-910(7) ("Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of a person's personal information is imperative.").

26. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES, (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/6BE8-HXBF?type=live]. The states that have not enacted data breach notification laws are South Dakota, New Mexico, and Alabama. *Id.*

27. *Id.*

28. GA. CODE ANN. § 10-1-912(a) (2009).

29. *Id.* § 10-1-911(2).

30. *Id.* § 10-1-911(3).

card, or debit card number; or (4) account passwords, PINs, or other access codes.[31] A "breach" occurs when a third party acquires, without authorization, a person's electronic data in a manner that "compromises the security, confidentiality, or integrity of personal information of such individual."[32]

If a breach occurs, then an information broker or data collector must notify affected persons "in the most expedient time possible and without unreasonable delay."[33] However, notice may be delayed if a law enforcement agency determines that the notification would compromise a criminal investigation.[34] Notice may be given in writing, via telephone, or through electronic media.[35] Substitute notice is available if the cost of notice to all affected individuals exceeds $50,000, if notice must be given to more than 100,000 people, or if the entity has insufficient contact information to provide written or telephonic notice.[36] Substitute notice requires a data collector or information broker to provide e-mail notice (if the entity has an e-mail address), conspicuously post notice of the breach on the entity's own website, and notify major statewide media of the breach.[37] No private cause of action exists in the statute.[38]

This Act has not resulted in a large amount of litigation. To date, only one published decision cites the Act.[39] Information on the number of breach notices required since the enactment of this law in 2005 appears to be unavailable.

2. California

California was the first state to enact a data breach notification law.[40] Since 2003, this law has served as a model for other states' data breach laws.[41] It requires any agency, business, or person doing business in California to notify a California resident if there has been a breach of that person's unencrypted personal information.[42]

Personal information is an individual's first initial or name and last name, together with: (1) the individual's social security number; (2) driver's license or state identification number; (3) an account, credit card, or debit card number; (4) medical information; or (5) health insurance information.[43] Alternatively, personal

---

31. *Id.* § 10-1-911(6).
32. *Id.* § 10-1-911(1).
33. *Id.* § 10-1-912(a).
34. *Id.* § 10-1-912(c).
35. *Id.* § 10-1-911(4).
36. *Id.* § 10-1-911(4)(D).
37. *Id.*
38. *See id.* § 10-1-910 to -915.
39. Willingham v. Global Payments, Inc., No. 1:12–CV–01157–RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013). *Solak v. The Home Depot* also references this statute. *See supra* note 23 and accompanying text.
40. CAL. CIV. CODE §§ 1798.29, .82 (West 2009 & Supp. 2015); Joerling, *supra* note 10, at 471.
41. Joerling, *supra* note 10, at 473.
42. CAL. CIV. CODE § 1798.29 (West 2009 & Supp. 2015) (agencies); *id.* § 1798.82 (persons or businesses); *see also* Joerling, *supra* note 10, at 471–72.
43. CAL. CIV. CODE § 1798.29 (West 2009 & Supp. 2015) (agencies); *id.* § 1798.82

information is also "[a] user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account."[44] A "breach" occurs when "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[45] The notification provisions of California's law contain identical language to Georgia's law.[46]

California, unlike Georgia, gives a private right of action to consumers for damages.[47] However, the efficacy of this cause of action is limited. Courts have interpreted the language of the statute to require a showing of actual damages.[48] The statute imposes liability only if an entity fails to notify California consumers in a timely manner, not for the breach itself.[49] Therefore, consumers must be able to connect the damages they allege to the breached entity's delayed notice.[50]

(persons or businesses).

44. *Id.* § 1798.29 (agencies); *id.* § 1798.82 (persons or businesses).

45. *Id.* § 1798.82(a).

46. *Id.* § 1798.29 (agencies); *id.* § 1798.82 (persons or businesses). The only two differences are that telephonic notice is not an option for notification under the California law and that the threshold requirements of costs and persons affected are higher for substitute notice in California.

47. *Id.* § 1798.84(b). Alternatively, an injunction is also available against "[a]ny business that violates, proposes to violate, or has violated" California's data breach law. *Id.* § 1798.84(e).

48. *See, e.g.*, *In re* Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 1009–10 (S.D. Cal. 2014). During this litigation the plaintiffs alleged that Sony should be responsible for paying, among other things, the fees to obtain credit monitoring services and the loss of value of the Sony consoles. *Id.* at 964–65. The court disagreed because other courts "have held that a plaintiff must allege actual damages flowing from the unreasonable delay (and not just the intrusion itself) in order to recover actual damages." *Id.* at 1010. Other federal courts have reached the same conclusion. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 638 (7th Cir. 2007) (dismissing plaintiffs' claims because future, anticipated harm is not sufficient to sustain a negligence action under Indiana law); Grigsby v. Valve Corp., No. C12-0553JLR, 2012 WL 5993755, at *2 (W.D. Wash. Nov. 14, 2012) ("[W]hen personal information is compromised due to a security breach, there is no cognizable harm absent actual fraud or identity theft."); Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 913–16 (N.D. Cal. 2009) (finding that an increased risk of identity theft cannot support a claim for actual damages); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1019–21 (D. Minn. 2006) (spending time and money to monitor credit for fraudulent activity does not satisfy the actual damage requirement).

49. *In re Sony*, 996 F. Supp. 2d at 1010 ("The statute does not penalize companies that simply suffer a security breach or fail to prevent an unauthorized third-party from acquiring their customers' personal information; rather, the statute penalizes companies that fail to disclose such incidents in the manner prescribed by the statute to affected state residents." (internal citations omitted)).

50. *Id.* (holding that in order to survive a motion to dismiss, "Plaintiffs [must] allege how the ten-day delay caused Howe to incur expenses for credit monitoring services, when these credit monitoring services were purchased, how the loss of use and value of Sony Online Services and Third Party Services were caused by the delay (and not the intrusion), and how Plaintiffs' Consoles diminished in value as a result of the delay.").

3. Indiana

Indiana's data breach statutes apply to state agencies and "data base owners," a term that covers both individuals and businesses.[51] A data base owner must notify an Indiana resident if the resident's unencrypted personal information "was or may have been acquired by an unauthorized person" or the resident's encrypted personal information may have been acquired by someone with the encryption key.[52] A state agency only needs to disclose a breach of unencrypted personal information.[53] A data base owner must also notify the Attorney General of any breach.[54] A state agency does not need to notify the Attorney General of a breach.[55] Otherwise, the provisions of notice are generally the same as the Georgia and California statutes.[56]

Significant differences exist between Indiana's data breach statutes and the statutes of Georgia and California. Indiana's statute defines "personal information" differently for state agencies and data base owners. For example, an individual's name must be associated with a social security number in order to be considered "personal information" for a state or local agency.[57] However, for data base owners, an unredacted or unencrypted social security number alone constitutes personal information.[58] Unlike California, Indiana does not include medical information or health insurance information in the definitions of personal information.[59] Notable notification compliance exceptions exist for data base owners.[60] Other provisions require the data base owner to develop and maintain "reasonable procedures" to protect the personal information of Indiana residents.[61] The statute also prohibits disposing of unredacted or unencrypted records without taking appropriate measures to make the records unusable to third parties.[62]

Actions for injunctions, civil penalties, and reasonable costs against data base owners are only available to the Attorney General.[63] In 2011, Indiana's Attorney General reached a settlement worth $100,000 with WellPoint, Inc. for delaying notice.[64] WellPoint also admitted fault, agreed to comply with Indiana's data breach

---

51. IND. CODE § 4-1-11-5 (2012) (agencies); *id.* § 24-4.9-2-3 (2007) (defining a "data base owner" as "a person that owns or licenses computerized data that includes personal information"); *id.* § 24-4.9-2-9 (2007) (defining a "person" as an individual or a business).

52. *Id.* § 24-4.9-3-1 (Supp. 2014).

53. *Id.* § 4-1-11-5(a) (2012).

54. *Id.* § 24-4.9-3-1(c) (Supp. 2014).

55. *Id.* § 4-1-11-5 (2012).

56. *See id.* § 4-1-11-8 to -9 (2012) (agencies); *id.* § 24-4.9-3-3 to -4 (2007 & Supp. 2014) (data base owners).

57. *Id.* § 4-1-11-3 (2012).

58. *Id.* § 24-4.9-2-10(1) (2007).

59. *Id.* § 4-1-11-3 (2012) (agencies); *id.* § 24-4.9-2-10 (2007) (data base owners).

60. *Id.* §§ 24-4.9-3-3.5 to -4 (2007 & Supp. 2014).

61. *Id.* § 24-4.9-3-3.5(b).

62. *Id.* § 24-4.9-3-3.5(c).

63. *Id.* §§ 24-4.9-3-3.5(d)–(e), 24-4.9-4-1(a); *see* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 n.8 (7th Cir. 2007) (noting that the exclusive remedy against a data base owner is an action by the Attorney General).

64. Press Release, Office of the Indiana Attorney General, Attorney General Reaches Settlement with WellPoint in Consumer Data Breach (July 5, 2011), *available at*

statute, offered free credit monitoring for two years for affected consumers, and offered to provide up to $50,000 of reimbursement to any customer who suffered losses due to the breach.[65] The Attorney General of Indiana has issued warning letters to at least forty-seven companies that have delayed issuing notice.[66]

In 2015, the Indiana legislature introduced Senate Bill 413, which would have overhauled Indiana's data protection laws.[67] Notably, Senate Bill 413 proposed a new section to the Indiana Code that defined "data" expansively. Senate Bill 413 defined data as "electronic or printed information that is collected, maintained, disseminated, or handled: (1) in a computerized format; (2) on paper; (3) on microfilm; or (4) in another medium."[68] Other changes to the terminology used in the Code were also included,[69] but other substantive protections would have been added if Senate Bill 413 were ratified. For example, Senate Bill 413 would have required online operators to delete data on Indiana residents once it is no longer being used for business purposes.[70] Data owners also would have been required to disclose to whom personal data was shared or sold and post this information in an online privacy policy.[71] The Indiana Attorney General would exclusively enforce violations of these provisions, but the penalty for noncompliance with the use of personal data would be up to a $1000 fine for each deceptive act.[72] Any failure to comply with the privacy policy provisions or a failure to properly dispose of data would carry a fine of either $5000 or $50 for each affected Indiana resident, whichever is greater, but the total may not exceed $150,000.[73]

B. The Consumer Privacy Protection Act of 2015

On April 30, 2015, Senator Patrick J. Leahy introduced the Consumer Privacy Protection Act of 2015 (CPPA) in the Senate.[74] An identical bill was introduced in

---

http://www.in.gov/portal/news_events/71252.htm [http://perma.cc/KA8R-5S92].

65. *Id.*

66. *Id.*

67. S.B. 413, 119th Gen. Assemb., 1st Reg. Sess. (Ind. 2015). The Indiana legislature failed to pass this bill, and it remains to be seen whether it will be reintroduced. *2015 Security Breach Legislation*, NAT'L CONF. STATE LEGISLATURES (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx [http://perma.cc/8C9X-45M2].

68. Ind. S.B. 413 § 4 (proposing a new section to the Indiana Code: § 24-4.9-2-2.7).

69. *E.g.*, *id.* § 7 (proposing a new section to the Indiana Code: § 24-4.9-2-3.2) (defining "data user").

70. *Id.* § 15 (proposing amendments to IND. CODE § 24-4.9-3-3.5). This section would require that a data user "retain sensitive personal information only as reasonably necessary" either for "a legitimate business, government, academic or nonprofit purpose" or for "compliance with applicable law." *Id.* (proposing amendment to IND. CODE § 24-4.9-3-3.5 (c)(1)). The data user also may not use personal information unless it is reasonably necessary for a legitimate purpose and the data subject has not opted out of the use. *Id.* (proposing amendment to IND. CODE § 24-4.9-3-3.5(c)(3)).

71. *Id.* (proposing amendments to IND. CODE § 24-4.9-3-3.5(b)(2), (e)).

72. *Id.* (proposing amendments to IND. CODE § 24-4.9-3-3.5(f)–(g)).

73. *Id.* (proposing amendments to IND. CODE § 24-4.9-3-3.5(h)–(j)).

74. S. 1158, 114th Cong. (2015). A substantially similar bill—the Personal Data Privacy

the House of Representatives.[75] The CPPA proposes criminal penalties for concealing a data breach and requires certain entities that collect information on at least 10,000 people to implement a security and privacy program that complies with standards articulated by the FTC.[76] Currently, the respective Senate and House bills are in committees.[77]

In the event of a security breach, "a covered entity shall . . . notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired."[78] Notice must also be given to the FTC.[79] A security breach occurs when there is reason to believe that there has been "unauthorized access to or acquisition of sensitive personally identifiable information."[80] Notice of a breach must be given "without unreasonable delay following the discovery" of the breach, which may not exceed thirty days unless an exception applies.[81] Written, telephonic, or electronic (e-mail) notice must be given to an affected individual, but if more than 5000 individuals in one state are affected by a security breach and personal notice is not possible, then a covered entity must notify major media outlets in the state of the breach and post notice in a "clear and conspicuous" place on its website.[82] The definition of "sensitive personally identifiable information" includes, inter alia, "[a] financial account number or credit or debit card number in combination with any security code, access code, or password."[83]

However, certain entities are exempted from the scope of the Act. Financial institutions, covered entities under HIPAA, and service providers of third-party electronic communications are excluded from the provisions of the CPPA.[84] In order

---

and Security Act of 2014—was introduced by Senator Leahy in the 113th Congress on January 8, 2014. This bill ultimately did not make it out of committees. S. 1897, 113th Cong. (2014).

75. H.R. 2977, 114th Cong. (2015).

76. S. 1158, 114th Cong. §§ 101, 201 (2015).

77. The Senate bill is in the Committee on the Judiciary. *Committees: S.1158—114th Congress (2015–16)*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/senate-bill/1158/committees [https://perma.cc/8X9G-TGRX]. The House bill is in the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. *Committees: H.R.2977—114th Congress (2015–16)*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/2977/committees [https://perma.cc/AQP6-TDLB]. No action has been taken on either bill since it was introduced.

78. S. 1158 § 211(a). This obligation extends to third parties that maintain systems or data on behalf of a covered entity. *Id.* § 211(b)(1).

79. *Id.* § 216.

80. *Id.* § 3(9)(A).

81. *Id.* § 211(c)(1)–(2).

82. *Id.* § 213. Telephonic notice may not be accomplished using a prerecorded message, and e-mail notice to an individual must not contain a request for personal information. *Id.*

83. *Id.* § 3(10). Other examples of "sensitive personally identifiable information" include a social security number, a driver's license number, a passport number, a unique electronic account identifier (such as an account number or username) in combination with a password or security question and answer, unique biometric data, information concerning an individual's geographic location, or password-protected digital photographs and videos. *Id.*

84. *Id.* § 201(c). A "service provider" is defined as "a business entity that provides electronic data transmission, routing, intermediate and transient storage, or connections to its

to be exempted from the CPPA, financial institutions must be in compliance with the requirements of the Gramm-Leach-Bliley Act, and covered entities under HIPAA and HITECH must be in compliance with the data security provisions of those regulations.[85]

Unlike the data breach notification laws, the CPPA would require businesses to take proactive measures. Businesses would be required to perform risk assessments to identify vulnerabilities to their data systems before they are breached.[86] Companies would also need to regularly assess and monitor their data privacy and security programs, including performing vulnerability testing and updating security programs in light of technological advances, threats, or changing business arrangements.[87] Additionally, there would be safe harbor provisions that could exempt an entity from the notice requirements. A breached entity would not need to identify consumers if it determines that any sensitive personally identifiable information is "rendered unusable, unreadable, or indecipherable" by the use of security technologies such as encryption, and that there is "no reasonable likelihood" that the breach will result in the data being misused.[88]

There is no private cause of action under the CPPA.[89] The Attorney General of the United States, the Attorneys General of the States, and the FTC have the right to enforce the provisions of the CPPA and seek injunctive relief and civil penalties.[90] The maximum that any entity can be fined under the CPPA is $5 million or the product of the number of persons affected and $16,500, whichever is fewer, for any violation, unless the violation is found to be "willful or intentional."[91] If a violation is found by a court to be either "willful or intentional," then the court may impose an additional penalty that is not to exceed $5 million.[92]

C. HIPAA and HITECH

HIPAA[93] and HITECH[94] provide the Department of Health and Human Services (HHS) with the ability to enact regulations protecting sensitive health information.[95]

---

system or network, where the business entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and the business entity transmits, routes, or provides connections for sensitive personally identifiable information in a manner that sensitive personally identifiable information is undifferentiated from other types of data that such business entity transmits, routes, or provides connections." *Id.* § 3(11).

85. *Id.* § 201(c)(1)–(2).

86. *Id.* § 202(a)(3)–(4).

87. *Id.* § 202(c), (e).

88. *Id.* § 212(b).

89. *Id.* § 204(b).

90. *Id.* §§ 203, 204, 218, 219.

91. *Id.* § 203(b)(1)–(2).

92. *Id.* § 203(b)(4).

93. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

94. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009).

95. *See* 45 C.F.R. pt. 160 (2014); *id.* pt. 164(A), (E).

These regulations apply to "covered entities" under the Act, which include health care providers who conduct covered health care transactions electronically, health plans, and health care clearinghouses.[96] HIPAA and HITECH contain a notice provision for all breaches of sensitive health information.[97]

The HHS has enacted five rules regarding the use of medical information.[98] HITECH strengthened the Privacy Rule, the Security Rule, and the Enforcement Rule.[99] In addition, the HHS modified the interpretation of HIPAA and HITECH in 2013.[100]

1. The Privacy Rule

The Privacy Rule requires covered entities under HIPAA to have safeguards in place to ensure the privacy of protected health information.[101] Protected health information is individually identifiable health information that is either transmitted or maintained in electronic or other media.[102] Covered entities must also have contracts with their business associates to ensure that the business associates safeguard protected health information.[103]

Covered entities may disclose or use an individual's protected health information without consent only if it is used for treatment, payment, or health care operations.[104] The general rule is that covered entities may not use or disclose protected health information without valid authorization.[105] Individuals may request that a covered entity not use or disclose health information, and if the entity agrees then it must adhere to its agreement absent exigent circumstances.[106] The amount of protected health information disclosed must always be the smallest amount necessary to achieve a given purpose.[107] Further, covered entities must notify individuals of the use of protected health information,[108] and the covered entity must have a designated privacy official and a contact person or office responsible for dealing with HIPAA complaints.[109] Moreover, all employees of a covered entity must receive training on how to properly protect and handle protected health information.[110]

---

96. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566, 5567 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164).

97. 42 U.S.C.A. § 17932 (West 2013).

98. *HIPAA Administrative Simplification Statute and Rules*, U.S. DEPARTMENT OF HEALTH & HUM. SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html [http://perma.cc/LEY8-DVTD].

99. *See infra* notes 101–142 and accompanying text. *See generally* 123 Stat. 226.

100. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5566.

101. 45 C.F.R. pt. 160 (2014); *id.* pt. 164(A), (E).

102. *Id.* § 160.103.

103. *Id.* § 160.102–.103.

104. *Id.* § 164.506(a).

105. *Id.* § 160.508(a)(1).

106. *Id.* § 164.502(c), .522(a).

107. *Id.* § 164.502(b).

108. *Id.* § 164.528.

109. *Id.* § 164.530(a).

110. *Id.* § 164.530(b).

2. The Security Rule

The Security Rule requires a covered entity to "protect against any reasonably anticipated threats or hazards to the security or integrity of" electronic protected health information.[111] HITECH extended the requirements of the Security Rule to covered entities' business associates, so that a business associate is no longer regulated by contractual employment agreements.[112]

HITECH's amendments to the Security Rule require notice of a data security breach in the event that an individual's unsecured protected health information is disclosed.[113] Unsecured information is simply information that is not encrypted or is otherwise usable.[114] Similar to the state data breach notification statutes, HITECH requires that affected individuals must be notified "without unreasonable delay" and that if a breach involving 500 people or more occurs, the covered entity must notify the media and the HHS.[115]

3. The Enforcement Rule

The Enforcement Rule establishes rules governing the compliance responsibilities of covered entities with respect to the enforcement process.[116] HIPAA states that the Secretary of the HHS "shall impose [a penalty] on any person who violates a provision of this part."[117] These penalties are tiered based on the mental knowledge of the breach by a covered entity. Four categories of mental knowledge exist: an entity did not know or could not have reasonably known a violation occurred; an entity had reasonable cause to know a violation occurred or would occur; an entity corrected a violation due to willful neglect; and an entity had a violation due to willful neglect that has not been corrected.[118] A violation by an entity that did not or could not have known of the violation is viewed as less egregious than a violation due to willful neglect, and the bands of monetary penalties reflect this reality.[119] Thus, a covered entity that does not know he or she violated HIPAA could pay as little as $100, while a violation due to willful neglect could result in a penalty as high as $50,000 per violation.[120] Maximum penalties for the total calendar year for these violations exist as well, so under no circumstances will a covered entity pay more than $1.5 million in a calendar year.[121]

The Secretary of the HHS will consider certain factors when determining if a penalty is warranted.[122] These factors include: the nature and extent of the violation,

---

111. *Id.* § 164.306(a)(2).
112. 42 U.S.C.A. § 17931(a) (West 2013).
113. *Id.* § 17932.
114. *Id.* § 17932(h).
115. *Id.* § 17932(d)(1), (e)(4).
116. 45 C.F.R. pt. 160(C)–(E) (2014).
117. 42 U.S.C.S. § 1320d-5(a) (Lexis 2008 & Supp. 2015).
118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.*
122. 45 C.F.R. §§ 160.404, .408 (2014).

including the number of persons affected; the nature and extent of the harm incurred; a history of prior compliance with regulations; and the financial condition of the covered entity, including the size of the covered entity.[123] No fine may be levied on a covered entity that demonstrates that its violation was not willful and that it has corrected the violation within thirty days of knowing (or within thirty days of the date the entity reasonably should have known) the violation occurred.[124] The Secretary has the right to waive any penalty that is incurred as the result of a nonwillful violation of HIPAA or HITECH "to the extent that the payment of the penalty would be excessive relative to the violation."[125]

4. 2013 Modifications to HIPAA and HITECH: The Final Omnibus Rule

On January 25, 2013, the HHS released its modifications to the HIPAA and HITECH rules.[126] These modifications, among other things, substantively changed the Privacy, Security, and Enforcement Rules and altered the HITECH breach notification requirements.[127]

The Privacy Rule now requires covered entities' business associates to use or disclose protected health information only as required by contract or pursuant to the HIPAA and HITECH regulations.[128] Business associates may also be held directly liable for violations of the Privacy or Security Rules.[129] The modifications also prohibit the sale of any protected health information without the affirmative consent of the individual.[130] Covered entities must redraft their privacy policies in response to these modifications and redistribute them to individuals.[131]

The Enforcement Rule is modified to incorporate the penalty structure from the HITECH Act.[132] Covered entities and business associates are now responsible for the acts of their agents.[133] The modifications also change the penalty structure so that any violation of HIPAA rules results in a penalty according to the proposed structure under HITECH.[134] The former maximum fine an entity could accrue in a single

---

123. *Id.* § 160.408.

124. *Id.* § 160.410(c).

125. *Id.* § 160.412.

126. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164).

127. *Id.* at 5566 ("This omnibus final rule is comprised of . . . [f]inal modifications to the HIPAA Privacy, Security, and Enforcement Rules . . . .").

128. *Id.* at 5570–76; *see also* 42 U.S.C.A. § 17934 (West 2013); 45 C.F.R. § 164.502(a)–(e) (2014).

129. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5566 ("Covered entities and business associates must comply with the applicable requirements of this final rule by September 23, 2013.").

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.* at 5581 ("[W]e believe that the notion that a principal is liable for the acts of its agent should not be an unfamiliar concept to covered entities and business associates."); *see* 45 C.F.R. § 160.402(c) (2014).

134. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5582–83; *see* 45 C.F.R. § 160.404 (2014).

calendar year was $25,000, but that has now changed to $1.5 million for all kinds of violations.[135] These penalties will be determined on a case-by-case basis[136] and certain affirmative defenses allow a covered entity to avoid a fine altogether.[137] The modifications also specifically list the factors the Secretary should examine when determining the proper civil monetary penalty.[138]

Additionally, the 2013 modifications altered HIPAA and HITECH regulations relating to notification requirements in the event that a covered entity suffers a data breach. An impermissible use or disclosure of protected health information is now presumed to be a breach unless the covered entity "demonstrates that there is a low probability that the protected health information has been compromised."[139] Previously, the interim final rule had required a covered entity to demonstrate that an individual was at no significant risk of harm in order to forego notice.[140] A covered entity now may demonstrate that there is a low probability that data has been compromised by assessing the risk of at least the following four factors: the nature and extent of the protected information involved, including the types of identifiers and risks of re-identification; the identity of the unauthorized user or viewer of the protected information; whether the protected information was actually acquired or viewed; and the extent to which risk to the information has been mitigated.[141] The modifications also strengthen the breached entity's duty to notify individuals that data has been obtained by an unauthorized third party.[142]

III. THE HOME DEPOT BREACH AS APPLIED

The Home Depot's data breach presents some difficult issues for the existing regime of state statutes. For example, many consumers would not even be able to bring a suit against the Home Depot for a variety of reasons.[143] Senator Leahy's proposed bill would be more effective than the variety of state laws, but it also would fail to provide an adequate remedy. However, if the Home Depot were subject to HIPAA and HITECH-style penalties, there may be more recourse available.

---

135. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5582–83; *see* 45 C.F.R. § 160.404 (2014).

136. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5583 ("[T]he Department will not impose the maximum penalty amount in all cases but will rather determine the amount of a penalty on a case-by-case basis.").

137. *Id.* at 5585–86; *see* 45 C.F.R. § 160.410 (2014) (listing affirmative defenses).

138. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5584–85; *see* 45 C.F.R. § 160.408 (2014).

139. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5641.

140. *Id.* at 5641–42 ("[B]reach notification is not required under the final rule if a covered entity or business associate, as applicable, demonstrates through a risk assessment that there is a low probability that the protected health information has been compromised, rather than demonstrate that there is no significant risk of harm to the individual as was provided under the interim final rule.").

141. *Id.* at 5642.

142. *Id.* at 5648 ("[I]t may be an 'unreasonable delay' to wait until the 60th day to provide notification.").

143. *See supra* note 38, 48–50, 63 and accompanying text; *infra* Part III.A.

A. State Breach Notification Laws

Good reason exists to believe that any suit filed against the Home Depot under the state data breach notification statutes will fail.[144] Georgia's statute only applies to "data collectors" and "information brokers."[145] The Home Depot is not a state entity, and therefore cannot qualify as a "data collector," nor can the Home Depot qualify as an "information broker" because it does not collect information for costs or fees.[146] Thus it would appear that Georgia's statute would not apply to the Home Depot. California's statute applies to businesses and would cover the Home Depot, as would Indiana's statute, which covers "data base owners."[147]

"Personal information" was compromised during the Home Depot breach. The definition of personal information covers an individual's name taken together with credit or debit card information.[148] Likewise, the loss of personal information qualifies as a "breach" under the state notification statutes. A "breach" occurs when an unauthorized person gains access to unencrypted personal information, which happened when individuals' card information was compromised by the malware in the Home Depot's system.[149]

The state notification statutes require the Home Depot merely to notify individuals of the breach of their data "without unreasonable delay."[150] The breach affected roughly fifty-six million cards, well above the threshold number that would require the company to notify statewide media and the State Attorneys General of the breach.[151] The Home Depot confirmed the initial breach through a press release and to major media outlets on September 8,[152] a mere six days after it was initially suspected.[153] The Home Depot also confirmed on September 18 that it had closed off the vulnerability in its system.[154] It also appears that the Home Depot has adequately

---

144. *See, e.g.*, Jeff Landis, *Home Depot Moves to Dismiss Data Breach Class Action*, ZWILLGEN BLOG (Oct. 17, 2014), http://blog.zwillgen.com/2014/10/17/home-depot-moves-dismiss-data-breach-class-action/ [http://perma.cc/4U28-7B8Y].

145. GA. CODE ANN. § 10-1-912 (2009).

146. *Id.* § 10-1-911(2)–(3).

147. CAL. CIV. CODE § 1798.82 (West 2009 & Supp. 2015); IND. CODE ANN. § 24-4.9-2-3 (2007) (defining a "data base owner" as "a person that owns or licenses computerized data that includes personal information"); *id.* § 24-4.9-2-9 (2007) (defining a "person" as an individual or a business).

148. *E.g.*, GA. CODE ANN. § 10-1-911(6) (2009); HAW. REV. STAT. § 487N-1 (Supp. 2015); 815 ILL. COMP. STAT. ANN. 530/5 (West Supp. 2015); KAN. STAT. ANN. § 50-7a01(g) (Supp. 2014); ME. REV. STAT. ANN. tit. 10, § 1347(6) (Supp. 2014); WIS. STAT. ANN. § 134.98(1)(b) (West 2009).

149. *E.g.*, CAL. CIV. CODE § 1798.82(a) (West 2009 & Supp. 2015).

150. *E.g.*, GA. CODE ANN. § 10-1-912(a) (2009).

151. The Home Depot, *supra* note 8; *see, e.g.*, IND. CODE ANN. § 24-4.9-3-1(b) (Supp. 2014).

152. Maggie McGrath, *Home Depot Confirms Data Breach, Investigating Transactions from April Onward*, FORBES (Sept. 8, 2014, 5:32 PM), http://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/ [http://perma.cc/E6U4-MB4V].

153. Krebs, *supra* note 6.

154. The Home Depot, *supra* note 8.

notified the State Attorneys General because there is no action pending against the Home Depot for failure to notify. This means no action against the Home Depot would exist in Indiana.

California's statute grants a private right of action to consumers, but it is unlikely that such actions will succeed.[155] Courts require plaintiffs to demonstrate there are actual damages that can be recovered.[156] However, the Home Depot has agreed to pay for fraudulent charges, together with the card-issuing banks, on the compromised cards.[157] The extra time that consumers must spend monitoring their credit and dealing with security issues is viewed as too speculative by the courts.[158] Unless the plaintiffs are able to show that they suffered actual identity theft or account fraud as a direct result of the Home Depot taking six days to confirm that a breach occurred, the courts are likely to dismiss any action.[159]

B. The Consumer Privacy Protection Act of 2015

The Home Depot would have been subject to some liability under the proposed Consumer Privacy Protection Act if it were law at the time of the breach. The Act applies to the Home Depot because it is a business entity engaged in interstate commerce that transmits sensitive personally identifying information.[160] The Home Depot would be required to take proactive security measures under section 202 of the Act[161] and would be required to notify individuals in the event of a breach of sensitive personally identifying information.[162]

A breach of sensitive personally identifiable information, as defined by the CPPA, would have occurred. The data's security and confidentiality was compromised, and a third party acquired the data without authorization.[163] Similarly, credit and debit card information was taken, which is one of the definitions of sensitive personally identifiable information.[164]

The Home Depot's potential liability would arise from its failure to take proactive security measures. Section 202 would require the Home Depot to identify potential vulnerabilities to its data systems and take adequate steps to protect against a breach.[165] Reports that the Home Depot was aware of the risks to its payment system may be sufficient to trigger liability under this section.[166] Further, the malware used in the Home Depot attack was a similar variant of the malware that breached Target's

---

155. *See* Landis, *supra* note 143; *see also supra* note 49 and accompanying text.

156. *See supra* note 48 and accompanying text.

157. The Home Depot, *supra* note 19.

158. *See supra* note 48 and accompanying text.

159. *See supra* notes 48–49 and accompanying text; *see also* Landis, *supra* note 143.

160. The Home Depot, *supra* note 8 (describing the Home Depot as "the world's largest home improvement specialty retailer" with over 2200 stores nationwide).

161. Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. § 202 (2015).

162. *Id.* § 211.

163. *Id.* § 3(9)(A).

164. *Id.* § 3(10)(B); *see* The Home Depot, *supra* note 8.

165. S. 1158, § 202(a), (c), (e).

166. S. 1158, § 202(a)(3)-(4) (outlining liability); Creswell & Perlroth, *supra* note 20 (reporting that the Home Depot knew of risks to its payment system).

systems six months earlier.[167] The Home Depot should have been able to take more proactive measures to guard against this kind of malware. Therefore, it is likely that the Home Depot would not be in compliance with section 202 and would be subject to an action for failure to adequately protect sensitive personally identifiable information.[168]

The Home Depot would likely not face liability for a failure to notify under the CPPA. The Home Depot confirmed that a breach had occurred within thirty days of first disclosing the possibility of a breach and presumably notified all affected individuals during that time period.[169] The Home Depot would have needed to notify individuals using a proper method of notice, such as by phone, mail, or e-mail.[170] The Home Depot would easily meet this requirement, as it took immediate steps to reach out to the affected individuals and notify them of the breach.[171] The breach affected, on average, over one million cards in each state, which may have triggered obligations for the Home Depot to notify major media outlets of the breach and to place notice on its website.[172] Again, the Home Depot confirmed the breach to major media outlets six days after the initial reports, easily within the thirty-day window provided for in the CPPA.[173]

Violations of section 202 are subject to an action by the U.S. Attorney General, the Federal Trade Commission, and State Attorneys General.[174] The maximum penalty that the Home Depot could incur for the breach under the CPPA is $5 million.[175] The Home Depot could be fined up to $5 million more if the violation is found by a court to be willful or intentional.[176] The Home Depot's violation of this section might be considered willful if the Home Depot was aware of the vulnerabilities to its system and neglected to rectify those vulnerabilities before the breach occurred.[177] However, given that the Home Depot did not actively disseminate the payment card information, it is more likely that it would not be considered to have willfully violated section 202, thereby capping the potential civil penalty at $5 million.[178]

---

167. *See* Krebs, *supra* note 20.

168. Under the enforcement provisions of sections 203 and 204, an action against the Home Depot could be brought by the U.S. Attorney General, the Federal Trade Commission, or the State Attorneys General. S. 1158, §§ 203–204. The maximum penalty that the Home Depot would be subjected to would be $5 million, although the number of affected credit and debit cards was approximately fifty-six million. *See* S. 1158 § 203(b)(2); Perlroth, *supra* note 12.

169. *See, e.g.*, McGrath, *supra* note 151.

170. S. 1158, §§ 211(a), 213(1).

171. *See Information Originally Posted in 2014: Customer Update on Data Breach*, THE HOME DEPOT, https://corporate.homedepot.com/mediacenter/pages/statement1.aspx [https://perma.cc/2MEC-J8VN].

172. S. 1158, § 213(2).

173. *See* McGrath, *supra* note 151.

174. S. 1158, §§ 203–204.

175. *Id.* § 203(b)(2).

176. *Id.* § 203(b)(3)–(4).

177. Creswell & Perlroth, *supra* note 20.

178. *See* S. 1158, § 203(b)(2); The Home Depot, *supra* note 8 (indicating that information was stolen).

The Home Depot's profits and sales make any fine of $5 million a drop in the bucket that is unlikely to incentivize different behavior. In fiscal year 2013, the Home Depot made $5.4 billion in profit on $78.8 billion in sales.[179] A fine of .0926% of annual profit seems like a slap on the wrist for the breach of such a large amount of sensitive personally identifiable information. However, it is possible that the Home Depot (or other companies that suffer a large-scale breach of data) would be able to negotiate a penalty that is substantially lower than $5 million. This is an attractive strategy for smaller companies that would not be able to afford to pay a larger fine without encountering financial difficulties, but the $5 million ceiling for nonwillful violations of section 202 will fail to motivate larger companies with billion-dollar profits because the fine represents such a low percentage of their total revenue.

C. HIPAA and HITECH

If the FTC adopted a nearly identical version of the HHS administrative rules governing HIPAA and HITECH, then the government would be able to levy a substantial fine on the Home Depot.[180]

The tiered penalty structure under the new modifications is applied when a covered entity violates one of the HHS regulations.[181] The Home Depot would likely fall into the band of penalties for "reasonable cause" or corrected willful neglect.[182] An entity would qualify for the reasonable cause band if, by exercising reasonable diligence, the entity would have known it violated an HHS rule.[183] Willful neglect means an entity had a "conscious, intentional failure or reckless indifference to the obligation to comply" with a rule.[184]

---

179. The Home Depot, *supra* note 8.

180. Currently the FTC is able to enforce provisions of the Federal Trade Commission Act, 15 U.S.C. § 41 (2012), and the Clayton Act, 15 U.S.C. § 12 (2012). *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMMISSION (Jul. 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/2NK9-GQHZ]. Under both the Federal Trade Commission Act (FTCA) and the Clayton Act, the FTC is able to seek injunctive relief for violations of its cease and desist orders. *Id.* The FTC can also seek equitable relief for reporting violations of the Clayton Act. *Id.* Civil damages actions by the FTC are available for violations of cease and desist orders under the FTCA ($16,000 per violation) and the Clayton Act ($5000 per violation). *Id.* Reporting violations under the Clayton Act can also be enforced by the FTC in an action for civil damages ($11,000 per violation). *Id.*

181. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566, 5582–83 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164).

182. *See supra* Part II.C.

183. 45 C.F.R. § 160.401 (2014). Other entities, such as the IRS, also distinguish between reasonable cause and willful neglect standards. IRC § 6724(a) (2012) states that "[n]o penalty shall be imposed under this part with respect to any failure if it is shown that such failure is due to reasonable cause and not to willful neglect." In order to demonstrate that reasonable cause exists, "a person must establish either that (1) there were certain specific mitigating factors with respect to the failure or (2) the failure arose from events beyond the person's control." 14A JEROME WAHLERT, MERTENS LAW OF FEDERAL INCOME TAX § 55:99, Westlaw (database updated Dec. 2015).

184. 45 C.F.R. § 160.401 (2014).

The Home Depot's failure to adequately prepare for the attack on its systems and subsequent breach, a "reasonably anticipated threat[] or hazard[] to the security and integrity of" electronic personal information, would be a violation of the Security Rule as defined by HIPAA (if the FTC were to adopt a similar rule for businesses).[185] The Home Depot failed to anticipate that a similar Target-style attack on its stores might occur using the same kind of malware.[186] If true, the reports that the Home Depot knew of the risks and ignored them would likely mean that Home Depot was willfully neglecting its security.[187] However, the Home Depot would have adequately met the notice requirements articulated under the HIPAA Privacy Rule and Security Rule as articulated in the modifications, because it notified people "without unreasonable delay" and within six days of becoming aware of the breach.[188]

The FTC would be free to impose penalties on the Home Depot under the willful neglect category. Under HIPAA and HITECH, these penalties can range from $10,000 to $50,000 per violation with a ceiling of $1.5 million for all violations.[189] The FTC would need to evaluate factors to determine the proper scope of the penalty.[190] The Home Depot would not be able to avail itself of the exclusion to monetary fines because its violation would be considered willful.[191] The FTC would see that the extent of the harm incurred as a result of the Home Depot's failure to secure its payment systems was immense, including fifty-six million cards, fifty-three million e-mail addresses, and up to $3 billion in fraudulent charges.[192] The financial condition of the Home Depot is such that it could pay a higher fine, given that it made $5.4 billion in profit during fiscal year 2013.[193] And given the size of the Home Depot's operations, including over 2000 stores in the United States alone, the factors would weigh in favor of the FTC levying a large fine on the Home Depot.[194] Thus, if the bands and ceilings of penalties stayed the same, the Home Depot would likely be fined up to $1.5 million for the data breach.

IV. PROPOSAL

The data security requirements on companies under current state statutes is woefully inadequate to give consumers a sense of protection and confidence. Pending

---

185. *Id.* § 164.306(a).

186. Krebs, *supra* note 20 (reporting that the same kind of malware used in the Home Depot breach was used to infiltrate Target's payment systems nearly six months prior to the Home Depot breach).

187. *See* 45 C.F.R. § 160.401 (2014).

188. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566, 5654 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164) ("[C]overed entities . . . must still provide notification of such breaches to affected individuals without unreasonable delay . . . .").

189. *Id.* at 5583; *see* 45 C.F.R. § 160.404 (2014).

190. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. at 5584–85; 45 C.F.R. § 160.408 (2014).

191. 45 C.F.R. § 160.410(c) (2014).

192. Team BillGuard, *supra* note 7; *see also* The Home Depot, *supra* note 8.

193. The Home Depot, *supra* note 8.

194. *Id.*

federal legislation is a step in the right direction but fails to properly incentivize companies because the penalty provisions are not strong enough. The FTC should immediately be given authority, as it would under the CPPA, to fine companies that fail to adequately secure and protect consumers' personally identifiable information.

The FTC should adopt the expectation that companies will "[p]rotect against any reasonably anticipated threats or hazards to the security and integrity of" personally identifiable information, including credit and debit card numbers, from HIPAA's Security Rule.[195] It also should adopt the requirements of the Privacy Rule, namely that all companies must train every employee on the proper handling of personal information. The bands of penalties found in the 2013 HIPAA and HITECH modifications and the Enforcement Rule should be applied to companies that fail to comply with the FTC's version of these rules. This would give the FTC the authority to fine companies that suffer data breaches due to security oversights based on the culpability level of the company. Further, the affirmative defenses offered by the modifications and the HIPAA Enforcement Rule should also be adopted so that a company will not be fined without willfully neglecting its security obligations. This prevents a system where businesses are subjected to strict liability for being the target of hackers with sophisticated malware. Additionally, a private cause of action is not ideal because granting such an action to consumers potentially holds companies liable for being a victim of a hack.

However, the current penalty bands should be reworked by the FTC, and each violation should have clearly marked parameters so businesses know what is expected if a data breach occurs. The monetary ceilings of the bands should be removed entirely, and the fine should be based on the same four factors used by the Secretary of the HHS: (1) the nature and extent of the breach, including the number of persons affected; (2) the nature and extent of the harm incurred; (3) whether the business has a history of prior compliance with regulations; and (4) the financial condition of the business, including the size of the business.[196] This will allow the FTC to properly fine companies based on culpability, the size of the breach, and the size of the company. Larger companies would pay heftier fines in order to incentivize compliance with the FTC regulations. The absence of a ceiling for violations ensures that a fine will not be a slap on the wrist. Rather, companies will seek to comply with the regulations to avoid the penalties and will not neglect the security of their systems.

CONCLUSION

The Home Depot breach of customer credit and debit card information illuminates the need for new regulations. The Home Depot allegedly failed to secure its payment systems properly, resulting in the breach of millions of consumer records, including e-mail addresses and payment card data. The ramifications from this breach for consumers and the Home Depot are immense. The Home Depot and other companies

195. 45 C.F.R. § 164.306(a)(2) (2014).

196. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566, 5584 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160, 164); *see* 45 C.F.R. § 160.408 (2014).

must be incentivized to properly secure customer data. State data breach notification statutes fail to do this because damages must be shown from the failure to notify properly. The Consumer Privacy Protection Act of 2015 proposed by Senator Leahy would be a step in the right direction, but the FTC should be given the power to fine companies that suffer breaches. The framework provided by HIPAA and HITECH better incentivizes covered entities' compliance with data security regulations. The FTC should adopt similar regulations immediately, including regulations based on HIPAA's Privacy, Security, and Enforcement Rules. Affirmative defenses and exceptions would ensure that a company is not being held strictly liable for being the target of hackers. But the FTC would be able to fine a company according to how culpable the company was in neglecting security measures, the size of the company, and history of compliance with similar regulations. Unlike current legislation, such a framework would effectively encourage companies' compliance with data security regulations and would result in a more proactive approach to data security from the private sector.