

July 2019

Identities Lost: Enacting Federal Law Mandating Disclosure & Notice After a Data Security Breach

John Ogle
University of Arkansas, Fayetteville

Follow this and additional works at: <https://scholarworks.uark.edu/alr>



Part of the [Business Organizations Law Commons](#), [Commercial Law Commons](#), [Consumer Protection Law Commons](#), [Legislation Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

John Ogle, *Identities Lost: Enacting Federal Law Mandating Disclosure & Notice After a Data Security Breach*, 72 Ark. L. Rev. 221 (2019).

Available at: <https://scholarworks.uark.edu/alr/vol72/iss1/7>

This Article is brought to you for free and open access by ScholarWorks@UARK. It has been accepted for inclusion in Arkansas Law Review by an authorized editor of ScholarWorks@UARK. For more information, please contact scholar@uark.edu.

Identities Lost: Enacting Federal Law Mandating Disclosure & Notice After a Data Security Breach*

I. INTRODUCTION: AN ABSENT STANDARD

Identity theft is real, it's here, and consumers need protection. Over the past five years hackers have stolen billions of consumers' sensitive information like social security numbers, addresses, and bank routing numbers from companies that have neglected their security measures.¹ Most of the time these security breaches are easily preventable.² Companies sometimes wait weeks, months, or even years to inform the customers whose information was stolen because there is no federal law that requires disclosure.³ As of 2018, all 50 states have adopted security breach notification laws that require companies to inform

* J.D. Candidate, 2019, University of Arkansas School of Law. The author sincerely thanks Professor Jonathan Marshfield for his insight and guidance, the staff of the Arkansas Law Review for their diligent editing assistance, his wife, mother, grandfather, and other family members whose constant support led to this comment's fruition.

1. See Rebecca Shabad, *Senate panel holds hearing on Equifax, YAHOO security breaches*, CBS NEWS, (Nov. 8, 2017, 12:30 PM) <https://www.cbsnews.com/live-news/senate-panel-holds-hearing-on-equifax-breach-consumer-data-security-live-updates> [<https://perma.cc/7P5E-EDJB>]; see also Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html> [<https://perma.cc/7JKQ-XHZ3>]; *Anthem to Pay Record \$115M to Settle Lawsuits over Data Breach*, NBC NEWS (June 23, 2017, 5:41 PM), <https://www.nbcnews.com/news/us-news/anthem-pay-record-115m-settle-lawsuits-over-data-breach-n776246> [<https://perma.cc/9584-7EZL>].

2. Cf. Liz Moyer, *Equifax's Then-CEO Waited Three Weeks to Inform Board of Massive Data Breach, Testimony Says*, CNBC: FINANCE (Oct. 2, 2017, 12:47 PM), <https://www.cnbc.com/2017/10/02/equifaxs-then-ceo-waited-three-weeks-to-inform-board-of-massive-data-breach-testimony-says.html> [<https://perma.cc/SKJ2-HFYP>] (discussing how Equifax knew about a weakness in its security platform and could have fixed it with a simple software update).

3. See Michael Rapoport & AnnaMaria Andriotis, *States Push Equifax to Explain Why It Took 6 Weeks to Disclose Hack*, WSJ (Oct. 28, 2017, 9:22 AM), <https://www.wsj.com/articles/states-push-equifax-to-explain-why-it-took-6-weeks-to-disclose-hack-1509196933> [<https://perma.cc/4KUZ-ACJ8>] (discussing how Equifax waited six weeks after discovery to disclose the breach to the public); see also Shabad, *supra* note 1 (YAHOO! waited three years after discovery to disclose the breach to affected customers).

consumers that their information may have been stolen after an attack,⁴ but there is no federal law enforcing such a requirement.⁵

Each state's law has different requirements with some requiring disclosure within 90 days, 45 days, 30 days, or the vague reference, "without undue delay."⁶ This lack of uniformity creates problems for businesses operating in multiple states because it remains uncertain how long they have to notify affected consumers. At no fault of their own, consumers are unaware and particularly vulnerable from the time the of the breach until they are notified. It is time for Congress to enact national legislation that will require companies to inform individuals whose personal information was stolen in a cyberattack within a uniform amount of time. Enacting a federal law with clear guidelines and mandatory disclosure requirements for companies affected by a breach would benefit consumers and businesses alike. Consumers would be better able to protect themselves from identity theft because they could secure credit monitoring services closer to the time of the breach. Companies would finally have a national standard to adhere to instead of 50 different state laws, some of which contain no specific disclosure requirement at all.⁷ This note seeks to provide a background of the current variance and lack of guidelines for data disclosure laws and explore the benefits of enacting federal legislation that would require a company to disclose a security breach to potentially affected consumers within a reasonable and uniform amount of time.

4. *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> [https://perma.cc/YBU2-Q4A8] (listing that Alabama and South Dakota both unanimously adopted data-security-breach notification law in the early part of 2018).

5. See Christopher Mims, *After Equifax, Should the Government Force Companies to Report Hacks?*, WSJ (Sept. 24, 2017, 8:00 AM), <https://www.wsj.com/articles/should-the-u-s-require-companies-to-report-breaches-1506254402> [https://perma.cc/JFS2-2WPV] (discussing proposed federal legislation that would have created a national standard for security-breach-disclosure protocols).

6. See *infra* Table 1.

7. Compare CONN. GEN. STAT. ANN. §36a-701b (West 2018) (requiring disclosure within 90 days), with ARK. CODE ANN. § 4-110-105 (West 2005) (urging disclosure within "the most expedient time and manner possible" but not imposing a specific requirement).

II. BACKGROUND: A REPETITIVE HISTORY AND LACK OF ACTION

In July 2017, internet hackers remotely accessed the credit reporting agency Equifax and stole the personal information of more than 100 million consumers.⁸ In addition to being one of the three main credit reporting agencies,⁹ Equifax also makes money selling credit monitoring and protection services.¹⁰ Hackers stole from Equifax more than half of Americans' personal information, including social security numbers, credit card information, account numbers, addresses, birthdates, bank routing numbers, and other information.¹¹ Perhaps the most infuriating aspect is that Equifax could have prevented the breach with a simple software update that was available months before the breach occurred.¹² Equifax chose not to disclose the breach to anyone until six weeks after the breach was discovered.¹³ After Equifax's IT department discovered the breach and notified Equifax's then CEO Richard Smith, Mr. Smith chose to wait three additional weeks to inform the board of directors.¹⁴ Although Equifax still maintains that no one, other than the CEO, knew of the breach until three weeks after it was discovered,¹⁵ evidence suggests that other corporate officers also knew.¹⁶ The

8. *See* Bernard et al., *supra* note 1.

9. *Id.*

10. *See id.*

11. *Id.*

12. *See* René Gielen, *Apache Struts Statement on Equifax Security Breach*, APACHE SOFTWARE FOUND. BLOG (Sept. 9, 2017), <https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax> [<https://perma.cc/SV5G-ZGGB>] (stating on behalf of the software company that Equifax uses that the access point used by the hackers was secured a month before the breach via a security update); *see also* Moyer, *supra* note 2 (Equifax executive's testimony shows that the company knew of the available fix to the weak point in the software, but never utilized the update).

13. Rapoport & Andriotis, *supra* note 3. Only six weeks after Equifax discovered the breach did they attempt to notify their customers and other potentially affected consumers. *Id.*

14. Moyer, *supra* note 2.

15. *See id.*

16. *See* Elizabeth Dexheimer, *Equifax Board to Review Executives' Stock Sales After Hack*, BLOOMBERG (Sept. 29, 2017, 1:53 PM), <https://www.bloomberg.com/news/articles/2017-09-29/equifax-board-to-review-executives-stock-sales-following-hack> [<https://perma.cc/6KR2-XZZS>] (full article on file with the Arkansas Law Review).

day after Mr. Smith supposedly learned of the breach, but still six weeks before public disclosure, Equifax CFO John Gamble and two other executives dumped their shares of Equifax stock equaling a combined \$1.8 million dollars.¹⁷ They are currently under DOJ investigation for insider trading.¹⁸

The effects of the Equifax security breach are far reaching. In fact, if you live in America, it is more likely than not that your personal information was stolen in the breach.¹⁹ But Equifax is not the first company to lose consumer information.²⁰ In 2013, hackers stole over three billion consumers' personal information from Internet giant YAHOO.²¹ Five years later, YAHOO has still not determined the source of the breach because internet hackers are often untraceable.²² Although Equifax lost more sensitive information, the YAHOO breach eclipsed the Equifax breach in sheer size.²³ As of 2018, YAHOO is still under government investigation.²⁴ At a recent Senate Hearing, Senator John Thune from South Dakota asked the former CEO of YAHOO, Marissa Mayer, why it took three years for the company to disclose the breach.²⁵ After avoiding the senator's question, making him re-ask it multiple times, Mayer finally answered that YAHOO did not know about the breach until November 2016, after which the

17. See *id.*; see also Tom Schoenberg et al., *Equifax Stock Sales Are the Focus of U.S. Criminal Probe*, BLOOMBERG (Sept. 18, 2017, 9:30 AM), <https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe> [<https://perma.cc/PJD8-Q7XF>] (full article on file with the Arkansas Law Review).

18. Schoenberg et al., *supra* note 17.

19. Mims, *supra* note 5.

20. See Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1233 (2017); see also Reed Ableson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES (Feb. 5, 2015), <https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html> [<https://perma.cc/B9R5-DB6E>] (discussing the Anthem and Staples cybersecurity breaches).

21. See Shabad, *supra* note 1 (noting that as of October 2017 YAHOO! executives confessed that all three billion accounts had been affected by the breach).

22. See *id.*

23. Hackers took from Equifax the “keys that unlock consumers’ medical histories, bank accounts, and employee accounts,” but YAHOO! lost the information of more user accounts. Bernard et al., *supra* note 1.

24. Cf. Shabad, *supra* note 1.

25. *Id.*

company quickly disclosed it to the public.²⁶ However, there is evidence that YAHOO knew about the breach at least several months or perhaps even years before November 2016.²⁷ YAHOO will likely pay heavily for its actions as a U.S. judge recently ruled that the data breach victims from the YAHOO security breach have standing to sue, and the company must face their litigation claims.²⁸

In 2015, hackers stole personal information from nearly 80 million account holders for the healthcare giant Anthem.²⁹ The healthcare company claimed that the attack did not access healthcare or financial information, but did steal account members' social security numbers.³⁰ After discovering the breach, Anthem immediately reported it to the appropriate regulatory authority several weeks before it was required to do so.³¹ After several years of battling multi-district class-action litigation, Anthem decided to settle all claims for \$115 million dollars without admitting fault or that any of its customers were adversely impacted from the breach.³² Although Anthem's security measures were breached, its quick disclosure and notification should be standard procedure in every data security breach.

Although only a few instances of data breaches are discussed in this article, many more companies have had their customers'

26. *Id.*

27. See Yanfang Ye, *Why Did YAHOO Take So Long to Disclose Its Massive Security Breach?*, THE CONVERSATION (September 30, 2016), <https://theconversation.com/why-did-yahoo-take-so-long-to-disclose-its-massive-security-breach-66014> [<https://perma.cc/26K6-FJE8>].

28. See Jonathan Stempel, *YAHOO Must Face Litigation by Data Breach Victims: U.S. Judge*, REUTERS (August 31, 2017), <https://www.reuters.com/article/us-verizon-yahoo-breach/yahoo-must-face-litigation-by-data-breach-victims-u-s-judge-idUSKCN1BB25Q> [<https://perma.cc/52FX-XXMF>]; see also *In re: Yahoo! Inc. Customer Data Security Breach Litigation*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *20 (N.D. Cal. Aug. 30, 2017).

29. See Abelson & Goldstein, *supra* note 20.

30. See *id.*

31. See *id.* (noting that an FBI spokesman said Anthem's immediate reporting of their security breach should serve as a "model" for other companies).

32. See Liz Freeman, *Anthem Settles a Security Breach Lawsuit Affecting 80M*, USA TODAY (June 26, 2017), <https://www.usatoday.com/story/money/business/2017/06/26/anthem-settles-security-breach-lawsuit-affecting-80m/103217152/> [<https://perma.cc/2ZSR-7LXL>].

information stolen, and most of the time, these companies end up paying little in fines or costs associated with the breach.³³

III. AVAILABLE REMEDIES

The current variance of the law takes away consumer choice. Affected consumers do not usually choose to independently acquire identity theft protection services because they do not know that they are at risk. They are at risk because there is no uniform law requiring notification within a set period. Therefore, the consumer must wait until the company decides to notify them of the breach to take action. The options available to an affected consumer are limited and inadequate. The current remedies are insufficient to protect the consumer because the stolen information is available for sale from the time of the breach until the consumer is notified and can choose to enroll in a credit monitoring service. An affected consumer has only a few options after notification: (A) enroll in free credit monitoring services from Equifax for one year, (B) file suit against the company individually, or (C) join a class action lawsuit. None of these remedies give the consumer what is most important – notification (soon after the breach) that their personal information is stolen and the opportunity to take action on their own.

A. IDENTITY PROTECTION SERVICE ENROLLMENT

A consumer can obtain Equifax free credit monitoring services for one year whether or not their information was stolen in the data security breach. In response to public outrage, Equifax has created a unique website—www.EquifaxSecurity2017.com—that enables consumers to determine if Equifax lost their information in the 2017 security breach and also provides consumers with free credit protection monitoring services for one year.³⁴ For a time, consumers were

33. See Josephine Wolff, *Why It's So Hard to Punish Companies for Data Breaches*, N.Y. TIMES (Oct. 16, 2018), <https://www.nytimes.com/2018/10/16/opinion/facebook-data-breach-regulation.html> [https://perma.cc/9P8C-TR6R].

34. See generally *2017 Cybersecurity Incident & Important Consumer Information*, EQUIFAX, <https://www.equifaxsecurity2017.com/> [https://perma.cc/DJ2X-XTWA] (last visited Feb. 20, 2019).

immediately notified and directed to this site when they accessed Equifax's main website, Equifax.com.³⁵ To determine if personal information was stolen in the breach, consumers are prompted to input information like their name and the last six digits of their social security number.³⁶ Equifax will provide credit protection services to any consumer, regardless of whether or not the consumer's information was stolen in the 2017 security breach.³⁷

Equifax offers multiple, free credit monitoring services like: an Equifax security report, credit monitoring on all three credit bureau sites, social security number monitoring on the dark web, \$1 million dollars of theft ID insurance that will help pay for expenses arising from identity theft, and allowing consumers to "freeze" their credit.³⁸ "Freezing" credit allows the consumer to prevent creditors from lending any credit in their name.³⁹ This tool would prevent an identity thief from using the customer's personal information to take out a loan, purchase on credit, etc.⁴⁰

Consumers are left vulnerable in perhaps their most critical time – from the time that the breach occurs until the time the company decides to disclose the breach to the public.⁴¹ The time immediately after the breach may be when hackers are most likely to sell consumers' information on the dark web, before either the company realizes that the breach has occurred or before consumers have been informed of the breach and of their need to obtain identity protection services. According to a 2017 Experian survey, only 18% of polled Americans were enrolled in a paid

35. See EQUIFAX, <https://www.equifax.com/personal/> [<https://web.archive.org/web/20171123173139/https://www.equifax.com/personal/>].

36. See *Getting Started*, EQUIFAX, <https://trustedidpremier.com/eligibility/eligibility.html> [<https://perma.cc/47CG-YNVJ>] (last visited Feb. 21, 2019). Author's note: After inputting my personal information into the Equifax website, Equifax told me that I was affected and my personal information had been lost in the breach.

37. See *generally* EQUIFAX, <https://www.equifax.com/personal/> [<https://perma.cc/L5JF-72GG>] (last visited Feb. 21, 2019).

38. See *Frequently Asked Questions – Cybersecurity Incident & Important Consumer Information*, EQUIFAX, <https://www.equifaxsecurity2017.com/frequently-asked-questions/#consumer-faqs> [<https://perma.cc/9TLX-KJBM>] (last visited Feb. 21, 2019).

39. See *id.*

40. See *id.*

41. See Hayley Tsukayama, *Why It Can Take So Long for Companies to Reveal Their Data Breaches*, WASH. POST (Sept. 8, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches/?noredirect=on&utm_term=.6b7274196d51 [<https://perma.cc/37LK-7L85>].

credit monitoring service.⁴² Because most Americans do not have identity theft protection services, thieves can sell the information online without the consumers' knowledge, and the consumer will not be notified for weeks or even months while the company is deciding when to inform consumers of a breach.⁴³ This window of opportunity gives thieves time to sell the stolen information before affected consumers know that their information has been stolen or have a chance or to obtain any kind of identity protection service.⁴⁴ It took more than a month for Equifax to disclose the breach to the public,⁴⁵ and in some cases companies have taken years to disclose a breach.⁴⁶ Even though remedial identity protection services are beneficial to consumers, the service may be too little, too late.

B. SMALL CLAIMS SUIT

Many frustrated consumers have decided to file civil suits against Equifax in different courts across the nation.⁴⁷ But filing an individual lawsuit is difficult and time consuming for the average person to attempt on their own, and hiring an attorney to handle a claim against Equifax would likely prove expensive.⁴⁸ One Stanford graduate student has made this process easier and has created a website called donotpay.com that allows individuals to enter their personal information and automatically file a small

42. See *Survey Findings: Are Consumers Making It Easier for Identity Thieves?*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/survey-findings-are-consumers-making-it-easier-for-identity-thieves/> [<https://perma.cc/YL2U-DN34>] (last visited Feb. 21, 2019).

43. See Tsukayama, *supra* note 41.

44. See *id.*

45. See *id.*; see Moyer, *supra* note 2.

46. See Shabad, *supra* note 1.

47. See, e.g., Ethan Wolff-Mann, *A New Website Lets You Automatically Sue Equifax with a Click*, YAHOO! FINANCE (Sept. 11, 2017), <https://finance.yahoo.com/news/new-website-lets-automatically-sue-equifax-click-214730288.html> [<https://perma.cc/3MK6-NSAB>]; *Lawsuits Against Equifax Pile Up After Massive Data Breach*, REUTERS (Sept. 11, 2017), <https://www.reuters.com/article/us-equifax-cyber-lawsuits/lawsuits-against-equifax-pile-up-after-massive-data-breach-idUSKCN1BM2E3> [<https://perma.cc/6WEL-W35T>]; Ian Salisbury, *Wanna Sue Equifax? Here Are All Your Options*, MONEY (Sept. 22, 2017), <http://money.com/money/4949869/equifax-data-breach-lawsuits/> [<https://perma.cc/77MJ-A23S>].

48. See Wolff-Mann, *supra* note 47; see also Salisbury, *supra* note 47.

claims suit against Equifax in their home state.⁴⁹ Plaintiffs hope that this guerilla tactic will overwhelm Equifax, that Equifax will not show up to each suit, and the court would simply enter a default judgement in the plaintiff's favor.⁵⁰ If the suit were to actually be tried, plaintiffs would encounter the problem of proving actual harm.⁵¹ Even though plaintiffs could prove that Equifax lost their information in the breach, they would likely struggle to link monetary damages to the extent of their harm.⁵² Although an independent suit could be a solution for an effected consumer, the difficulties in filing and potential remedies are likely not worth the effort. Because linking damages to identity theft is so difficult to prove, it is important that the company promptly notify the consumer that their information was stolen so that they at least have the option to take independent action or secure credit monitoring services in order to best protect themselves.

C. CLASS ACTION LAWSUIT

Another potential remedy for consumers is the class action lawsuit. Class action law suits are easy to join and are cost-free unlike individual suits.⁵³ A consumer would simply have to add his name to the lists of plaintiffs and sit back and wait for a check in the mail.⁵⁴ Chicago attorney Jay Edelson estimates that Equifax will have to settle their class action lawsuits for upwards of \$1 billion dollars.⁵⁵ This estimate is astronomically high compared to past settlement amounts that companies have paid for losing consumer information in a data breach, but Edelson notes that this case could be different due to the involvement of

49. See DONOTPAY.COM, <http://www.donotpay.com/> [<https://web.archive.org/web/20180109050700/http://www.donotpay.com/>]. Note: www.donotpay.com does not go to the actual website anymore but instead diverts to iTunes to download their app. See also Wolff-Mann, *supra* note 47; Salisbury, *supra* note 47.

50. See Wolff-Mann, *supra* note 47; Salisbury, *supra* note 47.

51. *Id.*

52. *See id.*

53. Salisbury, *supra* note 47.

54. *Id.*

55. Jeff John Roberts, *A Surprise in the Equifax Breach: Victims Likely to get Paid*, FORTUNE (Oct. 10, 2017), <http://fortune.com/2017/10/10/equifax-class-action/> [<https://perma.cc/Y6ME-52WW>].

multiple state attorneys general and the reluctance of courts to only grant free identity protection services as damages.⁵⁶

According to Equifax's last 10-Q report filed with the SEC in November of 2017, 240 class actions had been filed against the company only two months after the breach was disclosed.⁵⁷ Official numbers have not since been released but 76 more law suits have been granted class action status, transferred and consolidated to a court in Atlanta, Georgia where Equifax is located.⁵⁸ A class action was filed in Oregon almost immediately after the breach was announced asking for \$70 billion dollars in damages.⁵⁹ Although a \$70 billion dollar settlement certainly will not happen because Equifax simply cannot afford to pay that much, a record settlement may likely occur.⁶⁰ But even if Equifax did settle all claims for \$1 billion dollars, the 143 million affected consumers would only receive a negligible sum – less than ten dollars before attorney's fees are deducted.⁶¹ Although a class action could result in a costly settlement that would punish Equifax, consumers would see no benefit.

All of the potential remedies available to consumers are inadequate because the lack of a uniform, federal standard delays the notification to the affected consumers, which robs them of the opportunity to obtain protection on their own. A federal law requiring mandatory disclosure and consumer notification would benefit businesses and consumers. Consumers need to know that their information has been lost, likely within at least 30-45 days, to ensure that they can protect themselves from online thieves. This notification would also give them the opportunity to change

56. *Id.*; see also Francine McKenna, *Equifax Faces Its Biggest Litigation Threat From State Attorneys General*, MARKETWATCH (Sept. 15, 2017), <https://www.marketwatch.com/story/equifax-faces-its-biggest-litigation-threat-from-state-attorneys-general-2017-09-15> [<https://perma.cc/EY7X-NTTF>].

57. Equifax Inc., Quarterly Report (From 10-Q) (Nov. 9, 2017), available at <https://www.sec.gov/Archives/edgar/data/33185/000003318517000032/efx10q20170930.htm> [<https://perma.cc/VYH7-B94Z>].

58. *Lawsuits Filed Against Equifax Transferred to Another Court*, U.S. NEWS & WORLD REPORT (Dec. 18, 2017, 2:36 PM), <https://www.usnews.com/news/best-states/new-hampshire/articles/2017-12-18/lawsuits-filed-against-equifax-transferred-to-another-court>.

59. See McKenna *supra* note 56; see also Polly Mosendz, *Equifax Faces Multibillion-Dollar Lawsuit Over Hack*, BLOOMBERG (Sept. 8, 2017, 9:55 AM), <https://www.bloomberg.com/news/articles/2017-09-08/equifax-sued-over-massive-hack-in-multibillion-dollar-lawsuit>.

60. See Roberts, *supra* note 55.

61. See *id.*

some of their personal information online like financial account passwords and security questions.

IV. THE CURRENT STATE OF THE LAW

In 2018, South Dakota and Alabama legislatures both unanimously voted in favor of passing a data-security breach notification law, making them the last two states to do so. Both South Dakota and Alabama chose to include a notice requirement that requires companies to notify potentially affected consumers that their information may have been stolen within 45 days. The number of days for the disclosure requirement varies by state, which creates confusion for companies who have lost their customers' information. Attempting to solve this problem, United States congressmen have proposed federal legislation that would create a uniform notification requirement numerous times over the past decade in the United States House of Representatives, but no such bill has ever successfully passed.⁶² The European Union recently adopted a bill creating a standard for all included countries to follow.⁶³ Although the bill in the EU has many critics, the bill at least creates a uniform standard for all parties in that jurisdiction. Unlike the EU, American companies have no uniform standard to follow after a data security breach and must independently determine the correct protocol in each state. This inefficiency and confusion could be easily cured with a federal law that created a national standard.

A. STATE LEGISLATION

The variance of state law regarding data disclosure requirements after a security breach is extreme.⁶⁴ All 50 states have enacted some type of law that requires companies to disclose

62. See *infra* Section IV.C.

63. See *infra* note 102 and accompanying text.

64. See *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> [https://perma.cc/YG4Z-W8RV]; see also Selena Larson, *Senators Introduce Data Breach Disclosure Bill*, CNN, (Dec. 1, 2017, 10:51 AM), <http://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html> [https://perma.cc/37LU-N3DC]; Mims, *supra* note 5.

a data security breach to consumers.⁶⁵ The requirements vary greatly from state to state.⁶⁶ Forty states – Arkansas, California, Colorado, and Texas – have no specific disclosure requirement but urge disclosure “without unreasonable delay.”⁶⁷ Seven states – Alabama, Ohio, Rhode Island, South Dakota, Vermont, Washington, and Wisconsin – require a company that has learned of an internal data security breach to disclose the breach to the consumer “without unreasonable delay” but no later than 45 days after discovering the breach.⁶⁸ The state of Connecticut mandates disclosure within 90 days, Delaware requires disclosure within 60 days, and Florida has the shortest length of time before required disclosure with 30 days.⁶⁹

Many states, like Arkansas, have numerous exemptions that allow a company to further delay disclosure if certain requirements are met.⁷⁰ For example, in Arkansas, disclosure can be delayed if a law enforcement agency determines disclosure would inhibit a criminal investigation.⁷¹ Additionally, Arkansas allows a person or company not to disclose the data security breach if “after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.”⁷² This variance at the state level is alarming and makes it extremely difficult for multi-state companies to determine the appropriate course of action when dealing with a

65. *See supra* sources cited note 64.

66. *See supra* sources cited note 64.

67. *See e.g.* ARK. CODE ANN. § 4-110-105 (West 2018); CAL. CIV. CODE § 1798.29 (West 2018); COLO. REV. STAT. § 6-1-716 (West 2018); TEX. BUS. & COM. CODE §§ 521.002, 521.053 (West 2017).

68. *See* OHIO REV. CODE ANN. §§ 1347.12, 1349.19, 1349.191, 1349.192 (West 2018); R.I. GEN. LAWS ANN. §§ 11-49.3-1 et seq. (West 2018); VT. STAT. ANN. tit. 9, §§ 2430, 2435 (West 2018); WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (West 2018); WIS. STAT. ANN. § 134.98 (West 2017).

69. CONN. GEN. STAT. ANN. §§ 36a-701b, 4e-70 (West 2019); DEL. CODE ANN. tit. 6, § 12B-101 et seq. (West 2019); FLA. STAT. ANN. §§ 501.171, 282.0041, 282.318(2)(i) (West 2018).

70. *See e.g.* ARK. CODE ANN. § 4-110-105 (West 2018) prohibiting disclosure if a law enforcement agency determines that disclosure will inhibit a criminal investigation. Disclosure is contingent upon the law enforcement agency’s determination that disclosure will not inhibit the criminal investigation. *Id.* at § 4-110-105(c). If the person or business that is subject to the breach determines after a reasonable investigation that the breach is not likely to harm consumers, the person or business is not required to disclose the breach at all. *Id.* at § 4-110-105(d).

71. *See id.* at § 4-110-105(c).

72. *See id.* at § 4-110-105(d).

data security breach.⁷³ Often a company will simply not follow the law, like Equifax's six week delay after discovery to notify consumers of the breach, two weeks longer than Florida law requires.⁷⁴ Confusion about which state law to follow will likely continue until a federal law is enacted that will preempt state law and provide a uniform standard for companies and individuals to follow.

B. FEDERAL LEGISLATION

Currently there is no governing federal law that requires companies to report a data security breach to consumers.⁷⁵ The Fair Credit Reporting Act requires credit reporting agencies (CRAs) to inform consumers why they have been denied an extension of credit and their credit score. The Fair Credit Reporting Act also requires CRAs to delete or correct inaccurate information but does not require companies to disclose a data security breach to affected consumers.⁷⁶ 15 U.S.C. §§1681 c-1 allows a CRA to report or flag a consumer's account but only after the consumer provides notice that he suspects that his account has been hacked.⁷⁷ Neither of these acts provide consumers protection by forcing companies to disclose that they have been the subject of a data security breach.⁷⁸ Because there is no federal law to hold companies to a uniform standard, companies independently determine the requirements for each state.⁷⁹

73. See Joe Uchill, *Dem Reintroduces Breach Notification Law in Equifax Wake*, THE HILL, (Sept. 18, 2017, 11:24 AM), <http://thehill.com/policy/cybersecurity/351164-dem-reintroduces-national-breach-notification-law> [<https://perma.cc/SWF8-9ZAW>]; see also Larson, *supra* note 64; Mims, *supra* note 5. For companies with clients in many states, it is difficult and often expensive to determine which state laws to follow. See *id.*

74. FLA. STAT. ANN. §§ 501.171, 282.0041, 282.318(2)(i) (West 2018); see also Moyer, *supra* note 2.

75. See Mims, *supra* note 5; see also Larson, *supra* note 64.

76. FED. TRADE COMM'N, A SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT 2, <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> [<https://perma.cc/P6HU-TWWG>].

77. 15 U.S.C. § 1681c-1 (2017).

78. See 15 U.S.C. § 1681c-1 (placing fraud prevention responsibilities on the consumer).

79. See Stephen Embry, *State Data Breach Notification Laws Just got Crazier*, AMERICAN BAR ASSOCIATION: YOURABA, (June 27, 2018), <https://www.americanbar.org/news/abanews/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier/> [<https://perma.cc/JE3D-EMT7>] (noting the complexity of following varying state laws, especially in the period following a breach).

Enacting a uniform federal law that clearly identifies and explains a specific disclosure timeline would benefit consumers, creditors, governments, and businesses alike because all players would have one act to look to instead of 50 different ones.⁸⁰

C. FAILED LEGISLATION: THE PERSONAL DATA NOTIFICATION AND PROTECTION ACT

Legislation has been proposed numerous times that would create a uniform, federal notification standard for companies that have suffered a data-security breach.⁸¹ President Obama proposed the Personal Data Notification and Protection Act in 2015 that would have required companies that suffered a breach to notify consumers within 30 days of discovery.⁸² Under the act, individual notice can be delivered to the consumer through mail, telephone, or email.⁸³ Additionally, a company would be required to disclose the breach to the media if the number of individuals affected by the breach reached 5,000 in any one state.⁸⁴ The notice must include information pertaining to the nature of the breach, the type of information the company retained on the individual, and the contact information for the credit bureaus.⁸⁵

Different versions of this bill have often been introduced but have never passed.⁸⁶ Most recently in the wake of the Equifax breach, Representative Jim Langevin (D – RI) reintroduced a similar bill in December of 2017.⁸⁷ Representative Langevin noted,

80. *See id.*

81. Rachel German, *What Are the Chances for a Federal Breach Notification Law?*, THE UNIVERSITY OF TEXAS AT AUSTIN CENTER FOR IDENTITY: IDENTITY EXPERTS BLOG (last updated Aug. 18, 2015), <https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law> [<https://perma.cc/4FHF-MF85>]; *see also* Larson, *supra* note 64 (outlining federal bills that have been introduced governing security breaches); Uchill, *supra* note 73.

82. *See* Keith Gerver, *The Obama Administration's Personal Data Notification & Protection Act: An Analysis*, CADWALADER: CLIENTS & FRIENDS MEMOS (Feb. 12, 2015), <https://www.cadwalader.com/uploads/cfmemos/133cdc904f02d77cfd21dab2c0b62.pdf> [<https://perma.cc/WMR9-HMM5>] (summarizing the specific notice requirements provided in the proposed Act); *see also* German, *supra* note 81.

83. Gerver, *supra* note 82, at 5.

84. *Id.*

85. *Id.*

86. *Id.*; *see also* German, *supra* note 81; Larson, *supra* note 64; Uchill, *supra* note 73.

87. *See* Uchill, *supra* note 73.

There is much still to learn about the Equifax breach and its ramifications, what is abundantly clear, however, is that consumers are still not sure whether they were affected and what information was stolen. . . Equifax has done a terrible job communicating about the breach to date, and this legislation will ensure that any future such breach has a single standard and one federal regulator to help get actionable information to consumers quickly. While I do not believe that breach notification is the only legislative response required following Equifax, it is an important first step in building accountability and protecting consumers.⁸⁸

Similar legislation has failed for years mostly because states are unwilling to lose their enforcement powers because of a preempting federal law.⁸⁹ Each state has different qualifications and procedures for dealing with a data security breach and is reluctant to allow federal law to preempt.⁹⁰ After several congressional attempts to pass a federal data security breach law in 2015, forty-seven state attorneys general wrote a letter to congress requesting that the enforcement of data-security breach law be left to individual states.⁹¹ The letter stated,

State attorneys general are on the front lines responding to data breaches. Our offices hear directly from affected consumers, and we regularly respond directly to their complaints and calls. . . Preempting state law would make consumers less protected than they are right now. Our constituents are continually asking for greater protection. If states are limited by federal legislation, we will be unable to respond to their concerns.⁹²

Again in 2018, thirty-two state attorneys general signed a letter requesting that Congress not pass the Data Acquisition and

88. *Id.*

89. See German, *supra* note 81; see also Jesse Rifkin, *Data Security and Breach Notification Act would create the first-ever federal standard for penalizing hacks of consumer information*, GOVTRACK INSIDER (Dec. 22, 2017), <https://govtrackinsider.com/data-security-and-breach-notification-act-would-create-the-first-ever-federal-standard-for-9842596a27ba> [<https://perma.cc/A3P4-SPT9>] (noting concerns that federal law would lessen consumer protection).

90. See German, *supra* note 81.

91. Rifkin, *supra* note 89.

92. Letter from Nat'l Ass'n of Atty's Gen. to Congressional Leaders 4 (July 7, 2015), <https://atg.sd.gov/docs/Final%20NAAG%20Data%20Breach%20Sign%20On%20Letter.pdf> [<https://perma.cc/8BHH-WDH3>].

Technology Accountability Act (a similar version of prior bills but not containing a mandatory notification requirement) because the act takes away the states' enforcement powers and because the act:

allows entities suffering breaches to determine whether to notify consumers of a breach based on their own judgment of whether there is 'a reasonable risk that the breach of data security has resulted in identity theft, fraud, or economic loss to any consumer. . . .'⁹³

The letter goes on to argue that a federal agency will be much less equipped to handle the massive amounts of data-security breaches reported every day.⁹⁴ Representatives from each state will likely be reluctant to vote in favor of a bill that preempts their state's enforcement capabilities.⁹⁵ In 2015, Senator Dianne Feinstein (D – CA) voiced her support for a federal bill that would protect consumers, stating:

in just the last 18 months, many millions of Americans have had data stolen in hacks of Target, Neiman Marcus, Home Depot, Sony, JP Morgan Chase and other companies. Cyberattacks cost the economy hundreds of billions of dollars a year, and this will only get worse. Congress must take steps to minimize the damage.⁹⁶

Although similar legislation has failed for almost a decade, a federal law that simply required companies that have suffered a breach to notify potentially effected individuals rather than restricting state's enforcement capabilities may have a better chance of passing through the legislature.

93. Letter from Lisa Madigan, Ill. Att'y Gen., to Congressional Leaders 2 (Mar. 19, 2018)

http://www.illinoisattorneygeneral.gov/pressroom/2018_03/Committee_Leaders_letter.pdf [<https://perma.cc/VZ2P-ENBS>].

94. *Id.* at 4 (noting that over 21,000 breaches have been reported in Massachusetts since 2008, most only affecting 488 persons on average).

95. *See* German, *supra* note 81.

96. *Id.*

D. FOREIGN LAW: EU GENERAL DATA PROTECTION ACT

In April of 2016 the European Union passed the General Data Protection Regulation (“GDPR”).⁹⁷ The GDPR is a comprehensive act that covers many aspects of data security laws.⁹⁸ Article 33 of the GDPR provides that a business that has been the subject of a data breach must notify the appropriate regulatory authority within 72 hours of a breach.⁹⁹ Article 34 of the GDPR states that the company must notify the subject of the breach “without undue delay,” a provision also contained in many American state statutes.¹⁰⁰ Article 34 of the act provides three exceptions that do not require a company to report the breach to the affected consumer: (1) the data is encrypted, (2) “the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize,” and (3) it would involve disproportionate effort. In such a case, “there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.”¹⁰¹ Although the European Union has enacted a multi-national standard for all companies to abide by, the GDPR does not contain a specific disclosure requirement to affected individuals.¹⁰²

97. Regulation 2016/697, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN> [https://perma.cc/UFB2-R988].

98. *See id*; *see also* *GDPR Key Changes*, EUGDPR.ORG (last visited Feb. 22, 2019), <https://eugdpr.org/the-regulation/> [https://perma.cc/N4Y3-GE9Y].

99. George R. Lynch, *EU 72-Hour Breach Notice May Give Companies Headaches*, BLOOMBERG LAW PRIVACY AND DATA SECURITY (Sept. 6, 2016), <https://www.bna.com/eu-72hour-breach-n73014447213/> [https://perma.cc/R84G-XKMF].

100. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 52.

101. *Id.*

102. The GDPR requires disclosure to the appropriate regulatory agency, but only urges disclosure to the effected individual “without undue delay.” *Id.*

V. MOVING FORWARD

Internet hackers stole confidential information from more than 140 million Americans during the Equifax cyber security breach, a breach that could have easily been prevented.¹⁰³ Equifax was on notice that there was a weakness in their cyber security system, had the available patch to fix the problem, but somehow failed to implement a simple software update.¹⁰⁴ Many companies, not just Equifax, have suffered a data security breach where hackers have taken critical information that could allow the hacker to take out credit in the consumer's name, crippling their credit for almost a decade.¹⁰⁵ Companies have done little to fix the existing problem because prior companies that have suffered a breach have had to pay little for losing their customers' personal information.¹⁰⁶ The variance of state law makes it difficult for national companies to provide effective notice to potentially affected consumers within the statutory time frame.¹⁰⁷ It is far past time that the United States Congress pass a federal law requiring companies to disclose and notify potentially affected consumers after the discovery of a data security breach within a set time period.

Consumers, businesses, and regulatory agencies would all benefit from the creation of a uniform federal law requiring notification within a set time period. Consumers would benefit because federal law would require companies to notify them that their personal information may have been stolen. Giving consumers this notice would allow them to independently obtain credit protection services that could prevent or mitigate the consequences of identity theft. Business would benefit because a uniform, federal disclosure requirement would give businesses a

103. See *supra* notes 9-10 and accompanying text.

104. See *supra* notes 9-10 and accompanying text.

105. See *supra* note 31.

106. See *supra* notes 31, 33.

107. Companies that operate in multiple states will have different notice requirements for each state. See *infra* Table 1 (noting that some states have no specific disclosure time period because only include the phrase "without undue delay," while some states require notification to the potentially affected consumer within 90, 60, 45, or 30 days). See also *supra* notes 62-73 and accompanying text.

specific deadline within which to notify the consumer. Therefore, businesses could set up a standard procedure to deal with a data security breach, instead of devoting the critical man hours immediately after the breach to determine the 50 different disclosure requirements.¹⁰⁸ Federal regulatory agencies would benefit because they would have a single standard to enforce, making sure that a company that suffered a breach had adequately and sufficiently provided notice to the effected consumer.

Prior federal legislation has failed for a number of reasons. Corporations may be opposed to data disclosure laws because they would prefer a longer time period to internally assess the scope of the breach. The EU General Data Protection Act requires disclosure to the governmental agency, not the affected consumer, within 3 days of discovery¹⁰⁹ which may not be enough time for a company to even begin to understand the aspects, origin, and scope of the breach. State resistance is perhaps the primary reason federal law has failed. The majority of state attorneys general have joined together to show opposition to federal data security breach laws. Thirty-two attorneys general have signed a letter denouncing a proposed data security breach law currently in Congress. The letter is concerned that the states' enforcement powers will be restricted noting that it "appears to place Equifax and other consumer reporting agencies and financial institutions out of states' enforcement reach."¹¹⁰ In the letter, the attorneys general make an argument that no single federal agency is adequately equipped to handle the massive amounts of data security breaches reported to the offices of state attorneys general every day, and that is likely true. However, a federal law that simply required companies that have suffered a data security breach to notify the consumer whose personal information was lost within 30 or 45 days could still leave enforcement power with the states and also protect the individual. Creating a mandatory disclosure time line of 30 or 45 days would

108. See *infra* Table 1.

109. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 52.

110. Letter from Lisa Madigan, Att'y Gen., State of Ill. and 31 other state Att'y Gens. to U. S. House of Representatives Comm. on Fin. Servs. (March 19, 2018).

ensure that the consumer could obtain individual protection measures if they so desired.

Protecting the American consumer should be priority number one of the United States Congress. Individuals are unable to protect themselves if they do not even know that they are the victim of a security breach. It is imperative that federal law require companies to notify affected consumers about a data security breach so that the individual may obtain a credit monitoring service, especially because less than 20% of Americans are enrolled in a credit protection service at any given time.¹¹¹ Besides enacting a federal law containing a mandatory disclosure time limit for security breaches, Congress should create punishments for failing to disclose within the allotted time period. For instance, CEOs could be found criminally liable for failing to disclose a breach within the allotted time period. This would enforce accountability from the top down in every company, and likely help to ensure that consumers were quickly notified when their information was lost in a security breach. Mandatory settlements could be created for consumers for a company's failure to disclose a security breach within the allotted time. The settlements could include monetary sums or free credit report monitoring for an extended period of time or even for life. Fines could be enforced with a monetary penalty for each infraction. However, especially in a case like Equifax's where the company has hundreds of millions of customers' data,¹¹² a fine may result in a penalty that is too steep and would bankrupt the company.

VI. CONCLUSION

In the wake of the Equifax and numerous other internet security breaches, it is time for Congress to finally enact legislation that will protect American citizens. Unifying the 50 different state laws would provide a national standard that would benefit consumers, businesses, government regulators and cut costs. Protecting consumers and giving them adequate time to protect themselves before their information can be sold on the dark web is imperative. Maybe, after over a decade of failure, the

111. EXPERIAN, *supra* note 42.

112. Moyer, *supra* note 2.

United States Congress will finally pass a law that will at least require companies that have suffered a data-security breach to notify the potentially affected consumers within at least 30 days.

JOHN OGLE

Table 1:

State	Code Provision	Disclosure Time (Days)
Alabama	S. 318, 2018 Reg. Sess. (Ala. 2018)	< 45
Alaska	ALASKA STAT. ANN. § 45.48.010 (West 2018).	0
Arizona	ARIZ. REV. STAT. ANN. § 18-552 (2019).	0
Arkansas	ARK. CODE ANN. § 4-110-105 (West 2018).	0
California	CAL. CIV. CODE §§ 1798.29, .82 (West 2018).	0
Colorado	COLO. REV. STAT. § 6-1-716 (West 2018).	0
Connecticut	CONN. GEN STAT. ANN. §§ 36a-701b, 4e-70 (West 2019).	< 90
Delaware	DEL. CODE ANN. tit. 6, § 12B-102 (West 2019).	< 60
Florida	FLA. STAT. ANN. § 501.171 (West 2018).	< 30
Georgia	GA. CODE ANN. §§ 10-1-912, 46-5-214 (West 2018).	0
Hawaii	HAW. REV. STAT. ANN. § 487N-2 (West 2018).	0
Idaho	IDAHO CODE ANN. § 28-51-105 (West 2018).	0
Illinois	815 ILL. COMP. STAT. ANN. 530/1 (West 2018).	0
Indiana	IND. CODE ANN. § 4-1-11-5 (West 2018).	0
Iowa	IOWA CODE ANN. § 715C.2 (West 2019).	0
Kansas	KAN. STAT. ANN. § 50-7a02 (West 2018).	0
Kentucky	KY. REV. STAT. ANN. §§ 61.933, 365.732, (West 2018).	0
Louisiana	LA. STAT. ANN. § 51:3074 (2018).	0
Maine	ME. REV. STAT. ANN. tit. 10, § 1348 (2017).	0
Maryland	MD. CODE ANN., COM. LAW § 14-3504 (West 2018)	0
Massachusetts	MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2018).	0
Michigan	MICH. COMP. LAWS ANN. § 445.72 (West 2018).	0
Minnesota	MINN. STAT. ANN. § 325E.64 (West 2018).	0
Mississippi	MISS. CODE ANN. § 75-24-29 (West 2019).	0
Missouri	MO. ANN. STAT. § 407.1500 (West 2018).	0
Montana	Mont. Code Ann. §§ 2-6-1503, 30-14-1704, 33-19-321 (West 2017).	0
Nebraska	NEB. REV. STAT. ANN. § 87-803 (West 2018).	0
Nevada	NEV. REV. STAT. ANN. § 603A.220 (West 2017).	0
New Hampshire	N.H. Rev. Stat. Ann. § 359-C:20 (2018).	0
New Jersey	N.J. Stat. Ann. § 56:8-163 (West 2019).	0
New Mexico	H. R. 15, Leg. Sess. (N.M. 2017).	0
New York	N.Y. STATE. TECH. LAW § 208 (McKinney 2019);	0

2019

IDENTITIES LOST

243

	N.Y. GEN. BUS. LAW § 899-AA (McKinney 2019).	
North Carolina	N.C. GEN. STAT. ANN. § 75-65 (West 2018).	0
North Dakota	N.D. CENT. CODE ANN. §§ 51-30-02, -03 (West 2018).	0
Ohio	OHIO REV. CODE ANN. §§ 1347.12, 1349.19 (West 2018).	< 45
Oklahoma	OKLA. STAT. ANN. tit. 24, § 163 (West 2018).	0
Oregon	OR. REV. STAT. ANN. § 646A.604 (West 2018).	0
Pennsylvania	73 Pa. Stat. and Cons. Stat. Ann. § 2303 (West 2018).	0
Rhode Island	11, R.I. GEN. LAWS ANN. § 49.3-4 (West 2018).	< 45
South Carolina	S.C. CODE ANN. § 39-1-90 (2018).	0
South Dakota	S. 62, 2018 Leg. Assemb. (S.D. 2018).	< 45
Tennessee	TENN. CODE ANN. §§ 47-18-2107, 8-4-119, (West 2018).	0
Texas	TEX. BUS. & COM. CODE ANN. § 521.053 (West 2017).	0
Utah	UTAH CODE ANN. § 13-44-202 (West 2019).	0
Vermont	VT. STAT. ANN. tit. 9, § 2435 (West 2018).	< 45
Virginia	VA. CODE ANN. §§ 18.2-186.6, 32.1-127.1:05 (West 2018).	0
Washington	WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (West 2018).	< 45
West Virginia	W. VA. CODE ANN. § 46A-2A-102 (West 2018).	0
Wisconsin	WIS. STAT. ANN. § 134.98 (West 2018).	< 45
Wyoming	WYO. STAT. ANN. § 40-12-502 (West 2018).	0
District of Columbia	D.C. CODE ANN. § 28-3852 (West 2019).	0