Kansans at Risk: Strengthened Data Breach Notification Laws as a Deterrent to Reckless Data Storage

*Emily Matta**

I. INTRODUCTION

Data collection provides attractive opportunities for businesses to improve services, enhance marketing efforts, and generate revenue through data sharing practices.[1] As a result, businesses today are collecting mass quantities of data, leading to devastating data breaches.[2] Juniper Research projects that United States-based breaches will account for the majority of all data breaches in the world by 2023 because of data stockpiling practices.[3] Consumers, businesses, and lawmakers are struggling to adapt to an ever-changing technological landscape.

Today, data breaches are inevitable.[4] How can businesses address the threat of hackers with the means to change, adapt, and persist? Of course,

---

* J.D. 2020, University of Kansas School of Law, B.A. 2016, Wichita State University. I would like to thank my family for their unwavering support and the *Kansas Law Review* editorial staff for their patience and dedication. Of course, I would also like to thank the data breach notification I received in 2016, which finally scared me into diversifying my passwords and regularly checking my credit score.

1. Adam C. Uzialko, *How Businesses Are Collecting Data (And What They're Doing with It)*, BUS. NEWS DAILY (Aug. 3, 2018, 7:25 AM), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/JQG5-53RR]; *see also* Mark Sangster, *2018 Trends Overview: Compliance, Privacy and Security Family Tree*, LAW.COM (Feb. 8, 2019, 12:25 PM), https://www.law.com/2019/02/08/2018-trends-overview-compliance-privacy-and-security-family-tree/ [https://perma.cc/WSX9-LMDP] ("[C]onsumer preferences and behaviors are the raw materials for big data analytics that become a commodity for sale.").

2. Sangster, *supra* note 1.

3. *10 Cyber Security Facts and Statistics for 2018*, SYMANTEC, https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html [https://perma.cc/A7MN-PW22] (last visited Jan. 20, 2019) (presenting statistics from a 2018 study done by Juniper Research, a marketing research specialist).

4. *See* Beth Givens, Executive Director of Privacy Rights Clearing House, *Data Breach Readiness and Follow-Up: Being Prepared for the Inevitable*, PRIVACY RIGHTS CLEARINGHOUSE (Sept. 18, 2014), https://www.privacyrights.org/blog/data-breach-readiness-and-follow-being-prepared-inevitable [https://perma.cc/XB9H-BLPQ] (stating that "[i]t's not a matter of IF – rather, it's a matter of WHEN a breach will happen.").

businesses that take protection of consumer data seriously may still fall victim to a breach. However, regulation is necessary to deter data-collecting entities that shrug their shoulders at the looming threat of a data breach and to incentivize preemptive action to safeguard consumer data. One common and effective form of data privacy regulation is state data breach notification statutes, which mandate notification to individual consumers when personal information is compromised. State breach notification statutes encourage businesses to invest more in data security through the threat of reputational harm and subsequent customer loss. Further, notification allows consumers the opportunity to mitigate or eliminate their risk of identity theft. The effectiveness of these statutes, then, hinges on: (1) whether they are strong enough to deter reckless data storage, and (2) whether they provide the consumer with adequate information so they can protect themselves from identity theft.

The Kansas Protection of Consumer Information ("KPCI") statutes governing data breach notification rank among the most lenient in the United States.[5] Mostly untouched since their enactment in 2006,[6] the KPCI statutes are antiquated in today's data-driven world, including only a narrow definition of "personal information"[7] and requiring entities to notify consumers within an unspecified time frame.[8] Further, the statutes do not specify what information businesses need to include in notifications.[9] Failure to strengthen notification requirements leaves Kansas's business infrastructure weak and consumers vulnerable.

In the past, Kansas data breach victims have sought remedy in federal court on diversity jurisdiction grounds.[10] However, no data breach litigation has reached the Kansas Appellate Court or Kansas Supreme Court. The barriers Kansas data breach victims face in bringing suit and the many possible causes of action they may assert are beyond the scope of this Note.

This Note instead explores the limitations of the KPCI statutes and proposes modifications. Part II of this Note provides a broad overview of

---

5. Ellen Zhang, *Do Your State Laws Protect You? The United States Data Breach Heatmap*, DIG. GUARDIAN: DATA INSIDER (Aug. 15, 2018), https://digitalguardian.com/blog/do-your-state-laws-protect-you-united-states-data-breach-heatmap [https://perma.cc/SGZ5-WVAB] (ranking notification laws in all fifty states and assigning Kansas a two out of five, with a rating of one being the least restrictive).

6. KAN. STAT. ANN. §§ 50-7a01–7a04 (Supp. 2017). Section 50-7a03, relating to destruction of consumer records, was repealed in 2016.

7. *Id.* § 50-7a01(g).

8. *Id.* § 50-7a02(a)–(h).

9. *Id.* § 50-7a02(a).

10. *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1158 (D. Minn. 2015).

recent national and Kansas data breaches, a survey of state notification laws, and an introduction to the KPCI statutes. Part III addresses why it is necessary to update the KPCI statutes and proposes expanding the definition of "personal information," setting a strict notification deadline, requiring notification to the Kansas attorney general, and prescribing the form and substance of notifications. These modifications would encourage businesses to closely scrutinize the data they gather, to invest more heavily in data security infrastructure, and to implement post-breach recovery systems. Armed with more detailed notifications, Kansas consumers can identify what steps they need to take to mitigate or eliminate their risk of identity theft.

II. BACKGROUND

While the number of breaches decreased in 2018, the Identity Theft Resource Center's ("ITRC") 2018 End-of-Year Data Breach Report found that the number of consumer records exposed increased by 126%.[11] In 2017, there were 1,632 total breaches exposing 197,612,748 records.[12] In 2018, there were 1,244 total breaches exposing a shocking 446,515,334 records.[13] Massive data breaches involving high-profile companies undoubtedly contribute to these numbers. For example, the recently revealed Marriott breach alone exposed 383 million records.[14] The breach was reported to authorities on November 30, 2018,[15] and involved a guest reservation database Marriott acquired in a 2014 acquisition of Starwood Hotels and Resorts Worldwide.[16] Although "one of the largest [data breaches] in history,"[17] the Marriott breach failed to unseat the 2013-2014

11. IDENTITY THEFT RESOURCE CTR., 2018 END-OF-YEAR DATA BREACH REPORT 9 (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf [https://perma.cc/H5LC-QSXZ] [hereinafter 2018 END-OF-YEAR DATA BREACH REPORT].

12. *Id.*

13. *Id.* Of the 1,244 breaches reported to the ITRC in 2018, only half reported how many records were exposed. *Id.*

14. *Id.* at 7.

15. Marriott Int'l, Inc., Current Report (Form 8-K) (Nov. 30, 2018), https://marriott.gcs-web.com/node/28301/html [https://perma.cc/8XGK-96WF].

16. David Volodzko, *Marriott Breach Exposes Far More Than Just Data*, FORBES (Dec. 4, 2018, 1:47 PM), https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#4817fd5a6297 [https://perma.cc/J986-JQ9Q].

17. Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting Up to 500 Million Guests*, WASH. POST (Nov. 30, 2018), https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/?noredirect=on&utm_term=.a7cccbafe75d [https://perma.cc/5BK7-RMXT].

Yahoo breach, which currently holds the record.[18] Yahoo did not formally disclose this breach until 2016 and 2017[19] and reported that "all 3 billion [Yahoo] accounts . . . " were likely affected.[20] Another high-profile breach was the 2017 Equifax breach, which exposed over 140 million Americans' highly sensitive information.[21]

Uber suffered its own data breach in 2016, compromising personal information for 57 million Uber users and 600,000 drivers.[22] The company attempted to conceal the breach from users and regulators, paying off hackers with $100,000 and requiring them to sign a non-disclosure agreement to avoid reputational harm and potential loss in valuation.[23] This strategy backfired. Uber recently reached a joint settlement with state attorneys general in all fifty states for $148 million.[24] Kansas's share was more than $730,000.[25] These breaches demonstrate the scale and scope of the data breach crisis. But this is only the beginning. In fact, International Business Machines projects larger, more sophisticated, and more frequent attacks in coming years.[26] In other words, the data breach problem is here to stay. How we choose to respond will impact businesses and consumers for the foreseeable future.

Other countries are sensitive to the immense threat data breaches pose

---

18. Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO (Dec. 20, 2018, 5:01 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/4KLE-8GUV].

19. Although technically two separate breaches, the events are commonly referred to as a single breach. *See* Matthew C. Solomon et al., *Failure to Disclose a Cybersecurity Breach*, HARV. L. SCH. F. ON CORP. GOVERNANCE AND FIN. REG. (May 17, 2018), https://corpgov.law.harvard.edu/2018/05/17/failure-to-disclose-a-cybersecurity-breach/ [https://perma.cc/B6LG-SZTK].

20. *Id.*

21. Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 17, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [https://perma.cc/45AB-V3K6].

22. Bill Chappell, *Uber Pays $148 Million Over Yearlong Cover-Up of Data Breach*, NAT'L PUB. RADIO (Sept. 27, 2018), https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach [https://perma.cc/7LVU-54LC].

23. Gabrielle Orum Hernández, *Uber's Data Breach Cover-Up Strategy May Be More Common Than You'd Think*, CONN. L. TRIB. (Nov. 30, 2017, 3:04 PM), https://www.law.com/ctlawtribune/sites/ctlawtribune/2017/11/30/ubers-data-breach-cover-up-strategy-may-be-more-common-than-youd-think/ [https://perma.cc/PS8Z-G466].

24. Ben Kochman, *Uber, States Strike $148M Deal to End Data Breach Dispute*, LAW360 (Sept. 26, 2018).

25. Katie Moore, *Uber to Pay Kansas More than $730,000 Following Data Breach*, TOPEKA CAP. J. (Sept. 28, 2018, 1:38 PM), https://www.cjonline.com/news/20180928/uber-to-pay-kansas-more-than-730000-following-data-breach [https://perma.cc/3BB9-H672].

26. Louis Columbus, *IBM's 2018 Data Breach Study Shows Why We're in a Zero Trust World Now*, FORBES (July 27, 2018), https://www.forbes.com/sites/louiscolumbus/2018/07/27/ibms-2018-data-breach-study-shows-why-were-in-a-zero-trust-world-now/#68a322ab68ed [https://perma.cc/M7B3-2YHZ].

to consumers. The European Union's ("EU") General Data Protection Regulation ("GDPR"), effective May 25, 2018, governs management of EU citizen data, breach notification, and penalties for failure to comply.[27] The GDPR requires notification to the affected consumer and to the European supervisory authority within seventy-two hours of discovering the breach.[28] In addition to notification, the GDPR requires entities to perform risk assessments and implement data security measures relative to the risk.[29] Entities face stiff penalties for GDPR violations—up to $10,000,000 or 2% of their worldwide annual revenue, whichever is greater.[30]

In the U.S., Congress has struggled to implement national reporting statutes and other broad-based enforcement measures.[31] There are several possible reasons for the continued struggle to pass these laws: technology is rapidly changing, making it difficult to delineate a standard of data care, and big tech companies regularly lobby against federal legislation regulating data security.[32] Current federal laws governing data breaches tend to be industry-specific, such as the Gramm-Leach-Bliley Act[33] and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[34] The primary buffer against reckless storage of consumer

---

27. *See* Commission 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 (EU) [hereinafter GDPR].

28. *Id.* art. 33(1).

29. *Id.* art. 32.

30. *Id.* art. 83.

31. *See generally* Brett V. Newman, Note, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, 2015 U. ILL. J.L. TECH. & POL'Y 437 (2015) (providing an overview of legislative attempts to enact federal data security laws). *See also* Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUT. & HIGH TECH. L.J. 63, 77–78 (Feb. 2011) (stating that national attempts to enact data breach notification laws have failed).

32. Michael Rapoport & AnnaMaria Andriotis, *Equifax Lobbied for Easier Regulation Before Data Breach*, WALL ST. J. (Sept. 11, 2017, 10:39 PM), https://www.wsj.com/articles/equifax-lobbied-for-easier-regulation-before-data-breach-1505169330 [https://perma.cc/22KR-KYQB] (detailing Equifax's attempt to lobby for less regulation and liability for credit reporting companies); Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html [https://perma.cc/3R22-TDYL] (detailing Facebook, Google, IBM, and Microsoft's efforts to lobby for federal legislation overriding California's strict data privacy laws and allowing tech companies more leeway in how they handle consumer data).

33. 15 U.S.C. §§ 6801–6809 (2012) (requiring financial institutions to protect sensitive information).

34. Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.) (1996) (enabling the Department of Health and Human Services to establish regulations for maintaining privacy and security of protected health information).

information is Section 5 of the Federal Trade Commission ("FTC") Act, but it is not always exercised against entities when a breach occurs.[35]

Enforcement may depend on administration priorities. As one journalist notes, the Consumer Financial Protection Bureau ("CFPB"), created to protect consumers from unfair financial business practices, "has been gutted [and] rendered toothless under the Trump administration."[36] After the massive 2017 Equifax data breach, neither the CFPB nor the FTC took any enforcement action against Equifax.[37]

High-profile data breaches and international focus on data security regulation have placed increased pressure on Congress to pass legislation in this area. Several competing bills were introduced in April, November, and December 2018 to address data security standards and breach notification.[38] Those in support of federal legislation believe the federal government is best equipped to regulate this area because of the often cross-jurisdictional nature of these incidents.[39] Entities gathering and maintaining multi-resident data are faced with a disjointed, patchwork of state laws addressing data security and breach, many of which define "data

---

35. 15 U.S.C. § 45(a)(1) (2012). Section 5 of the FTC Act has two prongs: (1) deceptive practices; and (2) unfair practices. *Id.* To act under the deceptive practices prong, the FTC must show that the company made "an affirmative representation about the level of security it provided." David C. Grossman, Comment, *Blaming the Victim: How FTC Data Security Enforcement Actions Make Companies and Consumers More Vulnerable to Hackers*, 23 GEO. MASON L. REV. 1283, 1302 (2016). Because of this limitation, the FTC primarily uses the unfair practices prong, which views the company's failure to implement "reasonable and appropriate" data security standards as presumptively unfair to consumers. *Id.* at 1303. Although the FTC has brought more enforcement actions over the years, there have been surprisingly few given the number of data security breaches that occur each year. As of June 2015, the FTC had only ever brought around fifty enforcement actions in the data breach context. *Id.* (citing FED. TRAD. COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf [https://perma.cc/2M45-QUWW]).

36. Glenn Fleishman, *Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says*, FORTUNE (Sept. 8, 2018), http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/ [https://perma.cc/SJ68-8NHQ].

37. *Id.*

38. The Data Care Act, introduced in December 2018, would "impose fiduciary duties on 'online service providers' that collect individually identifying data about users," would require them to "reasonably secure personally identifiable information" and notify users if systems were breached. Jeffrey Atteberry, *In-House Counsel: Keep an Eye on Proposed Federal Privacy Legislation*, LEGAL INTELLIGENCER (Feb. 6, 2019), https://advance.lexis.com/api/permalink/0b824b4b-0c09-49cc-b695-ce6ccf7b85a7/?context=1000516.

39. For example, the 2016 Uber data breach involved rider and driver data from every state. Kate Conger, *Uber Settles Data Breach Investigation for $148 Million*, N.Y. TIMES (Sept. 26, 2018, 4:35 PM), https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html [https://perma.cc/H8PV-QMH5]. *See* Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467, 486 (2010) (referring to the "patchwork" of state notification laws and proposing that a federal law is necessary for comprehensive coverage).

breach" and other key terms differently, set different breach notification parameters, and may or may not mandate security safeguards.[40] When a breach does occur, the costs businesses incur navigating this complex web of state laws can be prohibitive.

Another significant barrier to passage of federal legislation is the issue of preemption. In the absence of federal regulation, state legislatures have stepped into this regulating role primarily by implementing mandatory breach notification statutes.[41] Some jurisdictions, including Kansas, have gone further, imposing a statutory duty on businesses to use reasonable care in collecting, maintaining, and disposing of consumer information.[42] California passed the first breach notification law in 2003[43] and remains the trailblazer in data security and privacy regulation. It recently passed two novel pieces of legislation: the first requires "reasonable security feature[s]" for internet-connected devices,[44] such as fitness trackers, cars, and refrigerators, and the second gives consumers broad rights with respect to their own data (e.g., the right to know how their data is used, the right to request that a business delete their data, and the right to opt out of data selling practices).[45]

States arguably have a higher stake in regulating entities holding resident data and better understand the nature of their businesses and the needs of their residents.[46] Comfortable with the statutes they have had in place for years, many states staunchly oppose preemption.[47] In March 2018, thirty-two states' attorneys general signed a letter addressed to the

---

40. *See* BAKER & HOSTETLER LLP, *Breach Notification Law Interactive Map*, https://www.bakerlaw.com/BreachNotificationLawMap [https://perma.cc/BMS7-XF7N] (last visited Jan. 4, 2019) (highlighting the major differences between state notification laws).

41. *See id.*

42. *See* KAN. STAT. ANN. § 50-6,139b(b) (Supp. 2017).

43. Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law is not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, n. 10–11 (2003).

44. *See* CAL. CIV. CODE § 1798.91.04(a) (operative Jan. 1, 2020).

45. California's Consumer Privacy Act of 2018, which will go into effect starting January 1, 2020, grants consumers rights similar to the GDPR's data portability rights. CAL. CIV. CODE § 1798.100–1798.199.

46. Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 64 (2015). *See also* Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 8 N.C.L. REV. 267, 272 (arguing that "principles of federalism, preemption, and the inflexibility of federal law expose the feebleness of a federal approach for data protection.").

47. Letter from Lisa Madigan, Ill. Attorney Gen., to the Committee on Financial Services 2 (Mar. 19, 2018), http://www.illinoisattorneygeneral.gov/pressroom/2018_03/Committee_Leaders_letter.pdf [https://perma.cc/RF94-6VB7] (noting thirty-two attorneys general oppose federal legislation that would preempt state laws).

Committee on Financial Services in response to the proposed Data Acquisition and Technology Accountability and Security Act.[48] The letter, penned by Illinois Attorney General Lisa Madigan, asserted that states are better equipped to handle data breaches and enforce cybersecurity standards than the federal government because of their ability to investigate breaches, address the concerns of affected residents, and adapt legislation to changing technology.[49] Madigan expressed concern that the proposed legislation would only capture large, national breaches while "preventing attorneys general from learning of or addressing breaches that have a smaller national scale but nonetheless victimize our state residents."[50] As debates on the merits of federal data security regulation rage on, state statutes continue to provide direction to businesses and offer transparency to consumers. Section II.A explains why data breaches create such risk to consumers, and Section II.B discusses recent Kansas breaches and the Kansas legislature's response.

A. What is a Data Breach?

Although the definition varies by statute, the ITRC defines "data breach" as "an incident in which an individual name plus a social security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure."[51] Breaches occur in a variety of ways, but the five most common are: (1) hacking, (2) unauthorized access, (3) employee error and negligence, (4) accidental exposure, and (5) physical theft.[52] Hacking was the number one cause of data breaches in 2018—of 1,244 total breaches reported, 482 incidents were caused by hacking.[53] Hackers target data sources containing sensitive personal information, such as social security numbers, to open new credit card accounts, apply for loans, and commit other fraudulent acts.[54] Once a consumer's social security number is stolen, the only surefire way to protect against identity theft is to obtain a new social security number, which is extremely difficult.[55]

---

48. *Id.* at 1.

49. *Id.* at 2–3.

50. *Id.* at 3.

51. IDENTITY THEFT RES. CTR., *Data Breaches*, http://www.idtheftcenter.org/Data-Breaches/data-breaches [https://perma.cc/JA62-D2F7] (last visited Apr. 5, 2019).

52. 2018 END-OF-YEAR DATA BREACH REPORT, *supra* note 11, at 10.

53. *Id.* at 9–10.

54. Loren F. Selznick & Carolyn Lamacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?*, 13 J. BUS. & TECH. L. 217, 221–22 (2018).

55. Stephen Jones, Comment, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern*

Consumers are not the only ones harmed by data breaches. Breaches cost U.S. companies an average $7.91 million per year.[56] The Ponemon Institute estimates that businesses lose $148 per leaked record.[57] The U.S. also has the highest notification cost in the world at $740,000.[58] Juniper Research estimates that "data breaches will cost businesses [globally] a total of $8 trillion over the next five years."[59]

B. Why is this Important for Kansas?

Kansas has one of the most lenient data breach notification statutes in the country.[60] In its current form, the Kansas statute is of little help to businesses and consumers. Kansas should follow other states and expand the scope of data covered under the statute, adopt a set deadline by which notification must be given, and set guidelines for the substance of notifications.

Data security is on the Kansas Legislature's radar. In 2016, Kansas joined a number of states in adopting data security standards for any data-collecting entity.[61] The statute, treated as "part of and supplemental to the Kansas consumer protection act," is inconspicuously tucked away in the Kansas Roofing Registration Act.[62] It requires "holder[s] of personal information" (defined in the same way as the KPCI statutes) to: (1) "maintain reasonable procedures and practices appropriate to the nature of the information," (2) "exercise reasonable care to protect the personal information," and (3) "take reasonable steps to destroy" any records the

---

Approach to the Data-Security Crisis, 50 TEX. TECH L. REV. 783, 788 (2018).

56. PONEMON INST., 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 15 (2018), https://www.ibm.com/downloads/cas/861MNWN2 [https://perma.cc/7LF2-TSVE] [hereinafter 2018 COST OF A DATA BREACH STUDY].

57. *Id.* at 3.

58. *Id.* at 9 (explaining that "[t]hese costs include the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication setups").

59. Press Release, Juniper Research, Cybercrime to Cost Global Business Over $8 Trillion in the Next 5 Years (May 30, 2017), https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn [https://perma.cc/6RWC-SH4J].

60. Zhang, *supra* note 5.

61. In 2016, Arkansas, California, Connecticut, Florida, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah had laws establishing data security standards for businesses. *Data Security Laws: Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 4, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx. Since 2016, the following states have adopted laws establishing data security standards for private businesses: Alabama, Colorado, Delaware, Illinois, Kansas, Louisiana, Michigan, Nebraska, New Mexico, New York, South Carolina, Vermont, and Virginia. *Id.* KAN. STAT. ANN. § 50-6,139b (Supp. 2017) (tasking holders of personal information to exercise "reasonable care").

62. *Id.* § 50-6,139b(g).

holder does not intend to keep.[63] Violations of the statute are treated as "unconscionable acts[s] or practice[s] in violation of K.S.A. 50-627," the Kansas Consumer Protection Act.[64] The statute neither creates nor permits a private cause of action, reserving all actions for the attorney general.[65]

In addition, the Cybersecurity Act, enacted May 2018, created the Kansas Information Security Office and established an information technology executive council to address data security issues relating to executive branch agencies.[66] The Cybersecurity Act is likely a response to two recent breaches involving state agencies. On March 14, 2017, the Kansas Department of Commerce discovered and isolated a breach, caused by hackers, which exposed more than 5.5 million individuals' social security numbers from multiple states.[67] The hackers also exposed an additional 805,000 user accounts that did not contain social security numbers.[68] The breach cost the state $175,000 in legal services through December 31, 2017, and approximately $60,000 for an IT contract to identify the compromised user accounts and fix the coding error the hackers exploited.[69] The State agreed to pay "for up to a year of credit monitoring services for victims in nine of the [ten] affected states," though this is not required by Kansas law.[70]

The State's response to the breach has been criticized for its lack of transparency—the breach only came to light after the Kansas News Service filed a Kansas freedom of information request.[71] Further, out of the 5.5 million individuals affected by the breach, the Department of Commerce only emailed about 260,000 victims because "it did not have email addresses for all users."[72] The KPCI does not require entities to notify victims by mail or telephone.[73]

---

63. *Id.* § 50-6,139b(b)(1)–(2). "Holder of personal information . . . means a person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person." *Id.* § 50-6,139b(a)(1).

64. *Id.* § 50-6,139b(d).

65. *Id.* § 50-6,139b(e). The finer details and implications of this statute are beyond the scope of this Note.

66. KAN. STAT. ANN. § 75-7202 (Supp. 2017).

67. Celia Llopis-Jepsen, *Hackers of Kansas System Accessed Social Security Numbers of Millions in 10 States*, KCUR 89.3 (July 20, 2017), http://www.kcur.org/post/hackers-kansas-system-accessed-social-security-numbers-millions-10-states#stream/0 [https://perma.cc/UHR3-7S3C].

68. *Id.*

69. *Id.*

70. *Id.*

71. Ed Silverstein, *Response to Kansas Department of Commerce Breach Suggests 'Poor Behavior'*, LEGALTECH NEWS (July 27, 2017), https://advance.lexis.com/api/permalink/164fe0de-849c-455f-9e85-ceec3f681d05/?context=1000516.

72. Llopis-Jepsen, *supra* note 67.

73. *Id.*

On February 23, 2018, a breach of the Kansas Department of Aging and Disability Services revealed confidential health information.[74] The breach disclosed, among other things, names, social security numbers, birth dates, and Medicaid identification numbers.[75] An employee improperly disclosed the information in an email sent to multiple local contractors.[76] Democratic Representative Jeff Pittman, in a debate on the Kansas House floor, noted the inconsistencies in data security between state agencies, stating: "We are not doing a good job in terms of keeping our data secure."[77] With the Kansas Legislature's attention recently focused on data security and cybersecurity, now may be the best time to update the KPCI statutes. Other states' notification statutes may provide a sound model for such updates.

C. A Brief Survey of State Notification Laws

In the absence of uniform federal regulation, states have stepped in to offer greater protection to their citizens. The protection has primarily taken the form of notification statutes.[78] State notification statutes require companies, under particular circumstances, to inform consumers that their personal information has been or may have been exposed.[79] California pioneered the first data breach notification law in 2003,[80] designed to curb identity theft by warning data breach victims when their personal information is compromised.[81] Fourteen states followed suit, modeling their own breach notification laws after California's.[82] As of March 2018,

---

74. News Release, Kan. Dep't for Aging and Disability Servs., KDADS Notifies Consumers About Potential Breach of Protected Health Information (Mar. 1, 2018), https://www.kdads.ks.gov/media-center/news-releases/2018/03/01/kdads-notifies-consumers-about-potential-breach-of-protected-health-information [https://perma.cc/PPM2-QDB4].

75. Elizabeth Snell, *Reported Kansas PHI Data Breach Could Involve Info of 11K*, HEALTH IT SECURITY (Mar. 8, 2018), https://healthitsecurity.com/news/reported-kansas-phi-data-breach-could-involve-info-of-11k [https://perma.cc/2XNV-G6SK].

76. Stephen Koranda, *Kansas Aging Agency Spills Personal Information of 11,000 People*, KCUR 89.3 (Mar. 1, 2018), http://www.kcur.org/post/kansas-aging-agency-spills-personal-information-11000-people#stream/0 [https://perma.cc/Z35H-68BP].

77. *Id.*

78. *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1 [https://perma.cc/PB2J-9GFH].

79. *See, e.g.*, CAL. CIV. CODE § 1798.29 (Deering, LEXIS through 2019 Sess.); IOWA CODE ANN. § 715C.2 (LEXIS through 2018 Reg. Sess.); LA. REV. STAT. § 51:3074 (LEXIS through 2018 Leg.); NEB. REV. STAT. § 87-803 (LexisNexis, LEXIS through 2019 Reg. Sess.); WYO. STAT. ANN. § 40-12-501 (LEXIS through Mar. 31 of 2019 Gen. Sess.).

80. CAL. CIV. CODE § 1798.82 (Deering, LEXIS through 2019 Sess.).

81. *See* Skinner, *supra* note 43, at nn.10–11.

82. *See* RANDY GAINER, MEALEY'S PRIVACY REPORT: POTENTIAL BUSINESS LIABILITY FOR

all fifty states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have data breach notification laws.[83] Alabama and South Dakota were last to adopt such statutes in the wake of the Equifax breach and enactment of the GDPR.[84] Many states have since amended their notification statutes to expand the scope of information covered and implement or refine mandatory reporting deadlines.[85]

There is commonality between state notification statutes. For example, all fifty states and U.S. territories include an encryption safe harbor, meaning that entities do not have to notify consumers if compromised data was encrypted.[86] Significant variations do exist, however, between state notification statutes. This section explores those variations.

1. Defining "Personal Information"

State notification statutes differ in how they define "personal information" subject to notification if compromised. The narrowest definition of "personal information" is "[a]n individual's first name or first initial and last name" plus (1) social security number, (2) driver's license or identification card number, or (3) financial account number or credit or debit card number.[87] Thirty-three states, Washington D.C., and Puerto Rico, however, have expanded definitions of "personal information."[88] For example, fourteen states include unique biometric data as a protected data element, such as fingerprints, voice recognition, or retina scanning.[89]

FAILURE TO SECURE CONSUMER DATA (2005), https://advance.lexis.com/api/permalink/c923acfb-72b7-4232-b949-9f9508e3482d/?context=1000516 (noting that fourteen states "enacted notification statutes generally modeled on California's statute" in the span of a few months in 2005).

83. Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, DATA PROTECTION REP. (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/ [https://perma.cc/6W8N-55E9].

84. *See* Julie Hein, *Navigating the State Data Breach Laws? An Enhanced Resource is Available*, DATA PRIVACY MONITOR (Sept. 21, 2018), https://www.dataprivacymonitor.com/data-breach-notification-laws/navigating-the-state-data-breach-laws-an-enhanced-resource-is-available/ [https://perma.cc/22X9-KQ66].

85. Jeewon Kim Serrato et al., *supra* note 83.

86. *See* BAKER & HOSTETLER LLP, *supra* note 40.

87. *See id.* Kansas is classified as having a narrow definition. *Id.*

88. The following states have expanded definitions of "personal information": Alabama, Alaska, Arizona, Arkansas, California, Colorado, Delaware, Florida, Georgia, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Oregon, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Virginia, Wisconsin, and Wyoming. *See id.*

89. ARIZ. REV. STAT. § 18-551(7)(a)(i) & (11)(i) (LexisNexis, LEXIS through 2019 legislation); COLO. REV. STAT. § 6-1-716(1)(g)(I)(A) (LEXIS through 2018 legislation); DEL. CODE ANN. TIT. 6, § 12B-101(7)(a)(8) (LEXIS through 2018); 815 ILL. COMP. STAT. ANN. 530/5(1)(F) (LexisNexis,

Many states also include medical information, health insurance policy information, and online account information (e.g., usernames or emails, plus any passwords or security questions and answers).[90] Some states go even further and include passport number, taxpayer identification number, date of birth, and an individual's mother's maiden name.[91]

2. Whether Notice is Required Within a Specific Time Frame

Although early notification statutes did not specify set deadlines for breach notification,[92] states are increasingly amending statutes to include specific deadlines. Nineteen states now require notification within a set "window" after discovery of a breach.[93] Colorado and Florida have the strictest notification periods, requiring notification no later than thirty days after a breach discovery.[94] The most common notification period—adopted by Alabama, Arizona, New Mexico, Ohio, Oregon, Maryland,

---

LEXIS through P.A. 101-1 of 2019 Sess.); IOWA CODE ANN. § 715C.1(11)(a)(5) (LEXIS through 2018 Sess.); LA. STAT. ANN. § 51:3073(4)(a)(v) (LEXIS through 2018 legislation); MD. CODE ANN., COM. LAW § 14-3501(e)(1)(i)(6) (LexisNexis, LEXIS through 2018 Sess.); NEB. REV. STAT. Ann. § 87-802(5)(a)(v) (LEXIS through 2019 Sess.); N.M. STAT. ANN. § 57-12C-2 (LexisNexis, LEXIS through 2019 Sess.); N.C. GEN. STAT. § 14-113.20(b)(11) (LEXIS through S.L. 2018-145 of 2018 Sess.); OR. REV. STAT. § 646A.602(11)(a)(A)(v) (LEXIS through 2019 Sess.); S.D. CODIFIED LAWS § 22-40-19(4)(e) (LEXIS through Feb. 27, 2019 legislation); WIS. STAT. ANN. § 134.98(1)(b)(5) (LEXIS through 2017–2018 Sess.); WYO. STAT. ANN. § 6-3-901(b)(xiii) (LEXIS through Mar. 31, 2019 legislation).

90. MO. ANN. STAT. § 407.1500(1)(9)(e) & (f) (LEXIS through 2018 legislation) (including medical information and health insurance policy number); MONT. CODE ANN. § 30-14-1702 (LEXIS through Feb. 28, 2019 legislation) (including insurance policy numbers); NEB. REV. STAT. § 87-802(5) (LexisNexis, LEXIS 2019 Sess.) (including unique identification number or routing code, biometric data, username, email address, and passwords or security questions and answers); OR. REV. STAT. § 646A.602(11)(a)(A) (LEXIS through 2019 Sess.) (including passport number or other U.S.-issued identification number, biometric data, health insurance information, and medical information); S.D. CODIFIED LAWS § 22-40-19(4) & (5) (LEXIS through Feb. 27, 2019 legislation) (including health information and usernames and emails).

91. MONT. CODE ANN. § 30-14-1702(7) (LEXIS through 2019 Sess.) (including passport numbers); N.D. CENT. CODE § 51-30-01(4)(a) (LEXIS through 2019 Sess.) (including date of birth, mother's maiden name, medical information, health insurance information, digitized or electronic signature, identification number assigned by employer with security code, access code, or password); OR. REV. STAT. § 646A.602(11)(a)(A) (LEXIS through 2019 Sess.) (including passport number or other U.S.-issued identification number, biometric data, health insurance information, and medical information).

92. *See, e.g.*, CAL. CIV. CODE § 1798.82(a) (requiring disclosure "in the most expedient time possible and without unreasonable delay").

93. Alabama, Arizona, Colorado, Connecticut, Delaware, Florida, Maine, Maryland, Massachusetts, New Mexico, Ohio, Oregon, Rhode Island, South Dakota, Tennessee, Vermont, Virginia, Washington, and Wisconsin all require notification to consumers within a particular window after a breach is discovered. *See* BAKER & HOSTETLER LLP, *supra* note 40.

94. COLO. REV. STAT. ANN. § 6-1-716(2) (LEXIS through 2018 Sess.); FLA. STAT. ANN. § 501.171(3)(a) (LEXIS through 2018 Sess.).

Rhode Island, Tennessee, Vermont, Virginia, Washington, and Wisconsin—is within forty-five days of a breach discovery.[95] Delaware and South Dakota require notification within sixty days of a breach discovery,[96] and Connecticut has the longest enumerated deadline at ninety days.[97] The remaining states, including Kansas, do not specify a deadline, instead opting for general language requiring notification "in the most expedient time possible and without unreasonable delay."[98]

3. Whether Notice to the Attorney General or a State Agency is Required

Thirty-five states and Puerto Rico require entities to notify the attorney general after a breach occurs, under certain circumstances.[99] In New York and Virginia, for example, no matter the size of the breach, the entity must notify the attorney general if the breach includes personal information.[100] Missouri, however, only requires entities to notify the attorney general and consumer reporting agencies if 1,000 or more persons are affected by the breach.[101]

---

95. ALA. CODE § 8-38-5(b) (LexisNexis, LEXIS through 2019 Sess.); ARIZ. REV. STAT. § 18-552(B) (LexisNexis, LEXIS through 2019 Sess.); MD. CODE ANN., COM. LAW § 14-3504(b)(3) (LexisNexis, LEXIS through 2018 Reg. Sess.); N.M. STAT. ANN. § 57-12C-6(A) (LexisNexis, LEXIS through 2019 Sess.); OHIO REV. CODE ANN. §§ 1347.12(B)(2) (LexisNexis, LEXIS through file) (state agencies) & 1349.19(B)(2) (LexisNexis, LEXIS through file 172) (persons and businesses); OR. REV. STAT. ANN. § 646A.604(3)(a) (LEXIS through 2019 Sess.); R.I. GEN. LAWS § 11-49.3-4(a)(2) (2018) (LEXIS through Jan. 2019 Sess.); TENN. CODE ANN. § 47-18-2107(b) (LEXIS through 2019 Sess.); VT. STAT. ANN. TIT. 9, § 2435(b)(1) (LEXIS through 2017 Sess.); WASH. REV. CODE ANN. §§ 19.255.010(16) (LexisNexis, LEXIS through 2018 Sess.) & 42.56.590(15) (LexisNexis, LEXIS through 2018 Sess.); WIS. STAT. ANN. § 134.98(3)(a) (LEXIS through 2017–2018 Sess.).

96. DEL. CODE ANN. TIT. 6, § 12B-102(c) (LEXIS through 82 Del. Laws, ch. 4); S.D. CODIFIED LAWS § 22-40-20 (LEXIS through 2019 Sess.).

97. CONN. GEN. STAT. § 36A-701B(b)(1) (LEXIS through 2018 Sess.).

98. *See, e.g.*, KAN. STAT. ANN. § 50-7a02(a) (Supp. 2018). *See also* ALASKA STAT. § 45.48.010(a) (LEXIS through 2018 Sess.); CAL. CIV. CODE § 1798.82(a) ; N.Y. GEN. BUS. LAW § 899-aa(2) (Consol., LEXIS through 2019 Sess.); VA. CODE ANN. § 18.2-186.6(B) (LEXIS through 2018 Sess.).

99. The following states require notification to the attorney general: Alabama, Alaska, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Virginia, and Washington. *See* BAKER & HOSTETLER LLP, *supra* note 40.

100. N.Y. GEN. BUS. LAW § 899-aa(8)(a) (Consol., LEXIS through 2019 Sess.); VA. CODE ANN. §§ 18.2-186.6(B) (LEXIS through 2018 Sess.) & 32.1-127.1:05(B) (LEXIS through 2018 Sess.).

101. MO. REV. STAT. § 407.1500(2)(8) (LEXIS through 2018 legislation).

4. Whether a Private Cause of Action is Permitted

Sixteen states, Washington D.C., Puerto Rico, and the Virgin Islands all provide for a private cause of action.[102] All other states and Guam either do not explicitly provide a private cause of action or only allow suits brought by the attorney general.[103]

5. Whether a Form of Notification is Specified

Many states also specify what information must be included in notification to data breach victims. Generally, these requirements include: (1) name and contact information for the reporting entity, (2) the type of information disclosed, and (3) telephone numbers and addresses of major credit reporting agencies.[104] Some statutes provide more transparency, requiring: (1) a description of the breach, (2) approximate date of the breach, and (3) advice to the consumer to report suspected identity theft to law enforcement.[105] Twenty-four states, including Kansas, Washington D.C., and Guam have no specific content requirements.[106]

D. Kansas Protection of Consumer Information Statutes

Current Kansas notification statutes are lenient and do not adequately protect consumers or incentivize safe data security practices. This Section will introduce the KPCI data breach statutes to identify weaknesses.

The KPCI statutes were enacted in 2006 and have not been updated since.[107] The statutes require individuals, corporations, governments, and

---

102. Alaska, California, Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Texas, Virginia, and Washington provide for a private cause of action. *See* BAKER & HOSTETLER LLP, *supra* note 40.

103. *See, e.g.*, MO. REV. STAT. § 407.1500(4) (LEXIS through 2018 legislation); WYO. STAT. ANN. § 40-12-502(f) (LEXIS through 2019 Sess.).

104. *See, e.g.*, ARIZ. REV. STAT. ANN. § 18-552(E); WYO. STAT. ANN. § 40-12-502(e).

105. CAL. CIV. CODE § 1798.29(d) (requiring information on what happened, what information was involved, what the entity is doing to rectify the situation, what the consumer can do in the meantime, and additional information); COLO. REV. STAT. § 6-1-716(2)(a.2); D.C. CODE ANN. § 28-3852 (LEXIS through 2019 Sess.); HAW. REV. STAT. § 487N-2(d) (LexisNexis, LEXIS through 2018 Sess.); IOWA CODE § 715C.2(5) (LEXIS through 2018 Sess.); N.M. STAT. ANN. § 57-12C-7 (LexisNexis, LEXIS through 2019 Sess.); OR. REV. STAT. § 646A.604(5) (LEXIS through 2019 Sess.).

106. *See, e.g.*, ALASKA STAT. § 45.48.010–.090 (LEXIS through 2018 legislation); IDAHO CODE § 28-51-105 (LEXIS through 2019 Sess.); KAN. STAT. ANN. § 50-7a01 (Supp. 2018); MONT. CODE ANN. §§ 30-14-1701-02 & 1704 (LEXIS through 2019 Sess.); UTAH CODE ANN. § 13-44-202 (LexisNexis, LEXIS through 2018); TIT. 9 GUAM CODE ANN. § 48.30 (LEXIS through P.L. 34-130).

107. KAN. STAT. ANN. § 50-7a01–50-7a04 (Supp. 2018).

other entities that conduct business in Kansas and own, license, or maintain consumer information to "conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused" after discovering a breach.[108] The statutes, however, provide no guidance for what constitutes a "reasonable and prompt investigation." The KPCI statutes also narrowly define "personal information," as a consumer's first name or first initial and last name plus any one or more of the following unencrypted or unredacted data elements: (1) social security number, (2) driver's license number or state identification card number, or (3) financial account number, or credit or debit card number.[109]

Notice is only required if the investigation "determines that the misuse of information has occurred or is reasonably likely to occur."[110] Essentially, entities must first perform a risk-assessment. If the entity determines that there is a high risk of misuse, it must give notice "as soon as possible to the affected Kansas resident . . . in the most expedient time possible and without unreasonable delay."[111] This vague standard leaves Kansas consumers unaware that their data has been compromised for an undisclosed period of time.

Even if notice is required, the KPCI statutes do not specify what information should be included in notification to Kansas consumers. The form of notification is also lax. The statutes define "notice" as "(1) written notice; (2) electronic notice . . .; or (3) substitute notice . . . ."[112] Substitute notice requires email notice, conspicuous posting on the entity's webpage, and "notification to major statewide media."[113] An entity may provide substitute notice if: (1) the cost of notice will exceed $100,000, (2) it needs to notify more than 5,000 people, or (3) it "does not have sufficient contact information to provide notice."[114] The State used substitute notice to notify Kansas consumers after the Department of Commerce's breach in 2017.[115]

Although the KPCI statutes do not provide an explicit private right of action for data breach victims,[116] the statutes do not foreclose the

108. *Id.* § 50-7a02(a).
109. *Id.* § 50-7a01(g)(1)-(3).
110. *Id.* § 50-7a02(a).
111. *Id.*
112. *Id.* § 50-7a01(c).
113. *Id.* § 50-7a01(e).
114. *Id.* § 50-7a01(c)(3).
115. Llopis-Jepsen, *supra* note 67.
116. *See* KAN. STAT. ANN. §§ 50-7a01–7a04.

possibility of a private remedy for violation. Section 50-7a02(g) provides that "[t]he provisions of this section are not exclusive and do not relieve an individual or commercial entity subject to this section from compliance with all other applicable provisions of the law."[117] This means that entities must comply with other federal and state laws governing data breaches, but it may also mean that other causes of action, such as an unfair or deceptive practices claim or negligence claim, are on the table. In the massive Target data breach litigation, the Minnesota District Court found the words "not exclusive" in the Kansas data breach notification statute to be sufficiently ambiguous to justify denying Target's motion to dismiss Kansas consumers' negligence claims.[118]

The breach notification statute could form the basis of a statutory duty to provide notification after a breach, enabling a private negligence claim if an unjustified delay in notification causes a data breach victim's injury. Aside from this, the attorney general may bring an action at law or in equity to enforce the provision and enjoin future violations.[119] However, enforcement by the attorney general is rare. The most notable example of attorney general enforcement is the Uber settlement, which the Kansas attorney general led on behalf of Kansas consumers.[120]

Lastly, the statutes include several safe harbors. First, encrypted or redacted data, if compromised, does not have to be reported at all.[121] This encourages entities to invest in data encryption to avoid the expenses of notification. Second, a state or federally-regulated entity that complies with the laws, regulations, or guidelines of its "primary or functional state or federal regulator is deemed to be in compliance with this section."[122] Third, notification in accordance with an entity's own procedures and policies, as long as they are "consistent with the timing requirements" of the statute, is sufficient to comply with this section.[123]

---

117. *Id.* § 50-7a02(g).

118. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014) (citing KAN. STAT. ANN. § 50-7a02(g)).

119. KAN. STAT. ANN. § 50-7a02(g). Analysis of the viability of such claims is beyond the scope of this Note.

120. Moore, *supra* note 25.

121. KAN. STAT. ANN. § 50-7a01(g).

122. *Id.* § 50-7a02(e).

123. *Id.* § 50-7a02(d).

III. ANALYSIS

A. Why Make Changes?

Consumers deserve to know when their personal information is compromised,[124] and the entities holding this data are in the best position to notify consumers. The primary purpose of data breach notification statutes "is to empower consumers" to take measures to secure their data post-breach.[125]

While data breaches can result in significant financial harm, few data breach victims suffer such harm. Rather, the primary consequence of a data breach is stress and loss of time and money spent monitoring credit, closing accounts, and addressing any red flags.[126] Banks and credit card issuers resolve many cases of fraud involving bank account and credit card information.[127] This creates another victim, however, as these institutions bear the incredible costs of issuing new bank cards and closing accounts.[128] For example, after the 2013 Target breach, banks and credit card issuers dished out approximately $172 million to reissue cards alone.[129] Aside from these forms of financial crime, the breach of highly confidential information leaves individuals open to identity theft. The Bureau of Justice Statistics estimated that 26 million individuals—or "10% of all U.S. residents age 16 or older"—reported an incident of identity theft in 2016.[130] Around 51% of identity theft victims did not discover the incident until "a financial institution contacted them about suspicious activity on their account."[131]

Breach notification laws, if done correctly, can provide consumers the time and information necessary to take protective action and reduce their risk of identity theft. Breach notifications also remind consumers to

---

124. Burdon, *supra* note 31, at 66.

125. LILLIAN ABLON ET AL., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 28 (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf [https://perma.cc/4YQ5-T2T8].

126. PONEMON INST., THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT 1 (2014), https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf [https://perma.cc/4RX7-NBEJ] [hereinafter THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT]. 76% of respondents reported feeling stressed after learning of a data breach involving their information. *Id.* at 6.

127. Tschider, *supra* note 46, at 50–51.

128. *Id.*

129. *Id.*

130. Erika Harrell, *Victims of Identity Theft*, U.S. DEP'T OF JUST. 1 (Jan. 2019), https://www.bjs.gov/content/pub/pdf/vit16.pdf [https://perma.cc/7P8R-GNK3].

131. *Id.* at 6.

carefully scrutinize who they provide their data to and to practice safe data security habits (for example, by diversifying passwords and regularly changing them). A study conducted by the Rand Corporation suggests that data breach notifications ultimately serve this purpose.[132] After receiving a data breach notification, 51% of respondents took protective action, including changing passwords or PIN numbers.[133] Respondents also indicated that they began "monitor[ing] credit card activity more closely," and requested new debit and credit cards.[134]

The Rand Corporation study also found that consumers want more regulation in this area. Surveyed respondents showed interest in seeing preventative measures to reduce the risk of future breaches, free credit monitoring services, and immediate notification to consumers once a breach occurs.[135] These measures were more likely to improve respondents' satisfaction following a breach than financial compensation.[136] A 2014 study, conducted by the Ponemon Institute, found that consumers want organizations to be required to provide identity theft protection, credit monitoring services, and compensatory relief through cash, products, or services.[137]

Data breach notification laws can also expose weak data security infrastructure and incentivize voluntary investment in data security. In a very real way, breach notification is a form of public shaming. The threats of public backlash and possible litigation raise the stakes for businesses and encourage preemptive action.[138] Broad privacy concerns from consumers and strict privacy regulations, such as the GDPR, have spurred increased investment in data security.[139] Gartner's recent research reported that worldwide spending on data security will "reach over $114 billion in 2018, an increase of 12.4% from last year."[140] Although

---

132. ABLON, ET AL., *supra* note 125, at 28–29.

133. *Id.* at 29.

134. *Id.* Other than change passwords or PIN numbers, 17% of respondents notified others of the breach, 4% began using a password manager, 13% stopped shopping at the reporting store or website, 24% switched or closed accounts, and 24% "Became More Diligent." *Id.* at 30 (detailed in Table 2.4). On the other hand, 22% of respondents took no action. *Id.*

135. *Id.* at 38 (detailed in Table 2.6).

136. *Id.*

137. THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT, *supra* note 126, at 1.

138. Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUS. L. REV. 1597, 1621–22 (2007).

139. Roger Aitken, *Global Information Security Spending To Exceed $124B In 2019, Privacy Concerns Driving Demand*, FORBES (Aug. 19, 2018, 1:28 PM), https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#68d518157112 [https://perma.cc/67VG-NULZ].

140. *Id.*

regulation increases the amount businesses have to spend on security, the improved infrastructure decreases businesses' costs once a breach occurs.[141]

Strict notification statutes provide additional incentives for businesses to invest in preventative measures. Increased spending and care can increase customer loyalty if consumers know that entities face costly and embarrassing notification in the event of a breach. Strict notification statutes also assure consumers that, should a breach occur, the entity must notify them promptly.

B. Concerns with Strict Regulation

Ponemon's 2018 study found that 48% of data breach incidents were caused by "malicious or criminal attacks."[142] Of all data breach incidents, these are the most costly to rectify at $157 per record.[143] The backbone of the opposition to heightened notification requirements rests in the notion that the hacker is a criminal, and the business or organization holding the information is the true victim.[144] This argument raises a serious question: who is responsible for the data, the business or the consumer? Some argue that consumers know the risk of data breaches and "voluntarily surrender at least some fraction of their security and privacy" when they choose to provide their information to an entity.[145] The publicity given to data breaches can support this contention. Consumers are aware that data breaches occur.

Strict regulation and statutory remedies place significant costs on businesses.[146] On average, businesses suffer an estimated $148 loss per leaked record.[147] Notification adds to these costs with activities such as creating contact databases, researching and complying with regulatory requirements, consulting with IT specialists (such as the IT contract Kansas entered after the Department of Commerce breach), paying for

---

141. Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get Over It!*, 19 SMU SCI. & TECH. L. REV. 3, 23 (2016).

142. 2018 COST OF DATA BREACH STUDY, *supra* note 56, at 9.

143. *Id.*

144. Riedy & Hanus, *supra* note 141, at 29 (stating that "[t]he cybercriminal who hacks the database and then sells or uses the data is the true culprit.").

145. *Id.* at 32.

146. *See, e.g.*, *id.* at 19–21 (discussing the immense costs businesses suffer as a result of breaches, including remediation costs of repairing and securing databases, networks, and equipment that may have been disrupted in the breach; clean-up costs associated with notifying victims of the breach and indirect costs such as customer churn; and post-breach costs including fines, penalties, and attorney's fees arising from litigation).

147. 2018 COST OF A DATA BREACH STUDY, *supra* note 56, at 3.

postage, and identifying secondary mail contacts.[148] When an entity suffers a breach involving thousands of records, the cost can become truly prohibitive, especially for small businesses. Meanwhile, the 2014 Ponemon study found that the average out-of-pocket cost to data breach victims was $38.[149] Additionally, 34% of the data breach victims surveyed stated that they were able to resolve problems resulting from the breach in one day.[150] Many argue that the consumer is therefore best equipped to bear these expenses. This argument, however, discounts the fact that the primary beneficiary of the data is the entity itself.

In addition to financial loss, businesses fear post-notification reputational harm. At one extreme, critics argue that businesses will make more effort to simply conceal breaches rather than comply with breach notification laws to prevent reputational harm and litigation, as Uber did in 2016.[151] This argument has some merit. A 2016 Symantec report found that more companies were not reporting the full extent of their data breaches.[152] At the other extreme, critics question whether strict regulation is necessary to deter businesses from unsafe data security practices, arguing instead that businesses already have an incentive to invest in data security to protect trade secrets and avoid the costs of a breach.[153]

A genuine concern is the effect such laws have on small businesses. Small businesses have fewer resources than larger companies to mitigate risk and respond to breaches.[154] Large entities rely on small business vendors, which hackers target for easy access to large enterprise data.[155] For example, a hacker caused the 2013 Target breach by gaining access to an HVAC contractor working with Targets' systems.[156] Small and midsize businesses are also attractive targets because cyber criminals can use

148. PONEMON INST., 2017 COST OF DATA BREACH STUDY: GLOBAL OVERVIEW 3 (2017), https://www.ibm.com/downloads/cas/ZYKLN2E3 [https://perma.cc/7WF9-Q44T].

149. THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT, *supra* note 126, at 7.

150. *Id.*

151. *See, e.g.*, Hernández, *supra* note 20 (discussing Uber's concealment of a 2016 data breach—"[d]isclosing data breaches tends to invite scrutiny from investors, open the door to litigation, and may not play well for a company's reputation.").

152. SYMANTEC, INTERNET SECURITY THREAT REPORT 6 (2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [https://perma.cc/KZ66-KAFF].

153. Riedy & Hanus, *supra* note 141, at 34 (the authors do not dispute the validity of data breach notification statutes, rather, they argue against civil liability for businesses).

154. Joseph Steinberg, *Small Businesses Beware: Half of all Cyber-Attacks Target You*, INC. (Mar. 21, 2017), https://www.inc.com/joseph-steinberg/small-businesses-beware-half-of-all-cyber-attacks-target-you.html [https://perma.cc/QH47-58JM].

155. *Id.*

156. *Id.*

automation to "mass produce attacks for little investment."[157] Lastly, small business owners tend to discount the value of investing in data security, believing that hackers only set their sights on large entities.[158] As a result, more hackers are targeting small businesses with 250 or less employees. As of March 2017, "half of all cyberattacks target[ed] small businesses."[159] Breaches can have profound effects on small businesses, which "are far more likely to fail as the result of a breach."[160]

Despite these concerns, businesses—often the primary beneficiaries of the data—should bear the costs of notification and take preventative action to avoid breaches. Businesses collect data to improve services and to attract more customers through targeted marketing campaigns. In addition, businesses have vast opportunities to sell consumer data to other companies, generating revenue. Because of increased data sharing practices, consumers are not in the best position to protect their personal information.[161] After voluntarily providing information to the initial entity, the consumer will not be notified if their information is sold or to who.

Although some scholars treat strict notification requirements as an unfair and unreasonable burden on business, fear of public outrage and the costs of notification have spurred preemptive investment in data security. This has had a profound impact on the technology sector, generating technological improvements, an expanding data security job base, better staffing, development of response plans, and greater employee awareness of how data breaches work and when a breach occurs.[162]

Advances in technology will also assist the cyber insurance market in adapting risk models. Although still in its infancy, the cyber insurance market is predicted to grow from $500 million a year to $3 billion a year by 2025.[163] There are unique difficulties in insuring against cyber risks because it is largely a recent development. There are few years of data to

157. Taylor Armerding, *Why Criminals Pick on Small Business*, CSO (Jan. 12, 2015, 4:04 AM), https://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html [https://perma.cc/DW4V-7HEP?type=image].

158. Steinberg, *supra* note 154.

159. *Id.*

160. *Id.*

161. *See* Tschider, *supra* note 46, at 46.

162. Larry Alton, *What Companies are Doing to Stop Data Breaches – Not Just React to Them*, TNW (Oct. 31, 2017), https://thenextweb.com/contributors/2017/10/31/companies-stop-data-breaches-not-just-react/ [https://perma.cc/GW49-B4VU].

163. Lucas Laursen, *Why Cyber Insurance Is a Smart Move for Business and Investors*, FORTUNE (Jan. 24, 2019), http://fortune.com/2019/01/24/cyber-insurance-boom/ [https://perma.cc/DC8N-RX6F].

build risk models off of and no two data breaches are exactly alike.[164] Increased investment may help develop risk models by creating an even larger market for cyber insurance. Increased investment in data security, in other words, fosters innovation in an ever-changing field. This not only benefits businesses and consumers, but also public institutions. Data breaches are not going anywhere. With time, they only grow in sophistication and breadth. As such, it is important that businesses develop data security infrastructure appropriate to the volume and type of data gathered.

The degree to which a business might experience reputational harm and the effects of customer churning (loss of customers after a data breach) are difficult to estimate. In past years, large data breaches, such as the 2012 Target breach, resulted in profound churning. Target's net earnings post-breach fell 46%.[165] In a 2017 Ponemon Report sponsored by Centrify, 31% of respondents discontinued their relationship with the company post-breach.[166] In contrast, the Equifax breach, one of the largest and highly-publicized breaches in history, temporarily hurt Equifax's position in the stock market, but it quickly recovered much of its losses.[167] Many predicted that the breach would be the impetus behind major changes to the credit-reporting industry.[168] Instead, little substantive change occurred, although Alabama and North Dakota both passed notification laws.[169] This absence of loss of business could be a result of Equifax's dominance in the credit-reporting industry. Low customer churn could also be a result of consumer apathy. Data breaches are now a common, unavoidable occurrence.

Regardless, businesses still fear the consequences of reputational harm, providing a powerful incentive for businesses to act preemptively by investing more in data security. Although increased spending does not necessarily correlate with a decrease in the number of data breaches, largely due to the increasing sophistication of hacking, it does decrease

164. *See* Ginger Szala & Janet Levaux, *Why Cyber Insurance Is Like the 'Wild Wild West': FinTech Insider*, THINKADVISOR (Jan. 23, 2019), https://www.thinkadvisor.com/2019/01/23/why-cyber-insurance-is-like-the-wild-wild-west-fintech-insider/?slreturn=20190026170938 [https://perma.cc/5KWA-ZW3F].

165. Hadley Malcolm, *Target Sees Drop in Customer Visits After Breach*, USA TODAY (Mar. 11, 2014, 11:51 AM), https://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/ [https://perma.cc/PV7A-7EA8].

166. PONEMON INST., THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE 12 (2017), https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf [https://perma.cc/4N8P-9DFD].

167. Fleishman, *supra* note 36.

168. *Id.*

169. *Id.*

business costs once a breach occurs.[170] In essence, it pays off to invest now. The 2018 Ponemon study found that a well-trained incident response team saved companies an average $14 per record.[171] The 2017 Ponemon report found that 113 companies experienced an average 5% decline in stock prices immediately after disclosure.[172] Companies, however, are less likely to see declining stock prices if they have strong data security infrastructure.[173] With strong infrastructure, companies are better able to respond to data breaches and see stock prices recover in an average of seven days.[174] In contrast, companies with poor data security infrastructure experience a slump in stock prices for more than ninety days.[175] Although businesses might be tempted to avoid reputational harm altogether by not notifying consumers, this is a risky decision. Businesses face potential suit by state attorneys general and even greater reputational harm, as Uber did for its 2016 data breach.[176]

Kansas currently has one of the most lenient breach notification laws in the country. This poses a significant risk to Kansas consumers and to Kansas businesses. Other states are strengthening their notification laws, causing businesses in those states to invest more in data security.[177] Increased investment strengthens data security and makes businesses in those states less attractive targets to hackers. Because of Kansas's lenient approach to notification, Kansas businesses may not invest as much as those in other states, and therefore make easier targets for hackers.

C. Proposed Changes

This Section suggests several alterations to the KPCI statutes, based on other states' models, to attain the ultimate purposes of data breach notification laws: (1) to provide enough information to Kansas consumers post-breach for them to protect themselves from financial crimes, and (2) to provide strong incentive to businesses to invest in data security. To achieve this purpose, it is necessary to expand the definition of "personal information," establish a set deadline for notifying consumers, require notification to the Attorney General, and stipulate the form and substance

170. Riedy & Hanus, *supra* note 141, at 23.
171. 2018 COST OF A DATA BREACH STUDY, *supra* note 56, at 3.
172. PONEMON INST., *supra* note 166, at 2.
173. *Id.*
174. *Id.*
175. *Id.*
176. Conger, *supra* note 39.
177. Tschider, *supra* note 46, at 68 (indicating that, over time, data breach notification laws have become increasingly strict).

of notification.

1. Providing a More Expansive Definition of "Personal Information"

Kansas currently defines "personal information" in an incredibly limited way, only requiring notification where name and either (1) social security number, (2) driver's license number or state identification card number, or (3) financial account, credit card or debit card number are included.[178] This narrow definition is likely a relic of the time the data breach notification statute was implemented—nearly fourteen years ago in 2006.[179] Since then, businesses have accumulated mass quantities of sensitive information, including biometric data, such as fingerprints, blood samples, faceprints, and iris scans.[180] Biometric data includes "some of the most sensitive forms of identification" due to its permanence.[181] Once captured, the victim can do little to avoid misuse, unlike passwords consumers can easily change or accounts they can easily close.[182] Because of the highly sensitive nature of biometric data, the definition of "personal information" in the KPCI statutes should include biometric data.

In addition to biometric data, the definition of "personal information" should include email addresses, passwords, and security questions and answers. Online accounts often contain highly sensitive information. Consumers access banking information online, file taxes online, pay rent and utilities online, and check credit scores online. Alternatively, the definition of "personal information" could include the basic data elements mentioned above and a catch-all, providing maximum flexibility. The catch-all could simply state "any information that, when combined with publicly available information, is reasonably likely to result in identity theft." A downside to a catch-all, however, is that it requires businesses to determine what data elements could leave consumers open to identity theft. Because of this ambiguity, the definition of "personal information" should include enumerated protected data elements.

Although some state notification laws include health information, inclusion of health information in the KPCI statutes would be detrimental. Entities holding protected health information are already subject to

178. KAN. STAT. ANN. § 50-7a01(g).

179. *Id.*

180. G.S. Hans, *Collection of Biometric Data Poses Serious Privacy and Personal Security Risks*, CDT (Jan. 26, 2016), https://cdt.org/blog/collection-of-biometric-data-poses-serious-privacy-and-personal-security/ [https://perma.cc/V7Q7-8QPG].

181. *Id.*

182. *Id.*

HIPAA regulation.[183] HIPAA requires notification to individuals with its own criteria, including a sixty-day notification period, adequately addressing any breach notification concerns.[184] Any added regulation in this field would place unnecessary difficulties on the many small, rural health clinics in Kansas.

2. Setting a Sixty-Day Notification Period

The current Kansas data breach notification statutes require notification "as soon as possible to the affected Kansas resident . . . . in the most expedient time possible and without unreasonable delay."[185] A notification period should be set in stone to encourage prompt action following a breach. Hackers act quickly after stealing data because they know they have a short window before the consumer realizes their data has been stolen.[186] Quick notification allows victims to monitor their credit, secure credit monitoring, and close or open new accounts where necessary.[187]

In theory, the current standard sounds reasonable, but it is vague. Entities might feel the need to react quickly, notifying consumers before identifying the source of the breach and ensuring that their networks are secure.[188] Alternatively, businesses may take their time in notifying consumers.[189] A set period gives businesses clear expectations of how quickly they need to respond and allows them to prioritize their post-breach activities accordingly.

Notification within sixty-days of identifying the breach is ideal. This gives businesses of all sizes ample time to identify the cause of the breach and secure data and restore systems before notifying those affected. This also discourages entities from taking their time in notifying consumers. Entities that fail to notify Kansas consumers within sixty-days, absent a criminal investigation or approval of the attorney general, would be subject to suit from the attorney general. In addition, entities that fail to notify consumers within sixty-days should be required to provide free credit-monitoring services to affected Kansas consumers for at least one year after notification. This is a fair penalty considering the heightened

183. *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/TAN7-JPFC] (last visited Apr. 5, 2019) (citing 45 C.F.R. §§ 164.400-414, the breach notification regulation).

184. *Id.*

185. KAN. STAT. ANN. § 50-7a02(a).

186. Tschider, *supra* note 46, at 70.

187. Rode, *supra* note 138, at 1624–25; Skinner, *supra* note 43, at 20.

188. Rode, *supra* note 138, at 1621–22.

189. *Id.*

risk Kansas consumers face the longer they remain unaware that their data has been compromised.

3. Requiring Notification to the Attorney General

Currently, entities experiencing a breach involving Kansas consumer information are not required to notify the Kansas attorney general. This is a missed opportunity. Notification to the Kansas attorney general would allow the attorney general to identify businesses and particular sectors that are frequent targets of attacks. This could shed light on weak data security infrastructure and highlight room for improvement. Notification to the Kansas attorney general would also help identify entities that are maintaining negligible data security standards subject to suit under K.S.A. § 50-6,139b. As such, entities suffering a breach should be required to notify the attorney general if 1,000 or more Kansas residents are affected, a common threshold in other state statutes.[190] Entities should notify the attorney general within sixty days of determining that a breach has occurred.

4. Indicating Form and Substance of Notification

The current Kansas data breach notification statute does not specify what information should be included in breach notifications to Kansas consumers. The statute should provide at least some guidance to entities after a breach. Alabama's statute, for example, is a strong model of what Kansas should require in notifications: (1) name and contact information for the reporting entity, (2) the type of information breached, (3) the actions the entity is taking to restore confidentiality, (4) the number and address for major credit reporting agencies, (5) the approximate date of the breach, and (6) advice to the consumer on what they can do to secure their data privacy and prevent identity theft.[191] Although some states require a description of the breach, including the cause, this information should not be required. If the entity was hacked, it may wish to include such information to minimize responsibility. Consumers may react more generously if the breach was caused by a malicious external attack rather than a negligent internal actor.

These notification requirements benefit both victims and entities. Without guidance on what to include in notifications, entities run the risk of including too little information and potentially subjecting themselves to

190. Tschider, *supra* note 46, at 71.

191. Edward A. Hosp et al., *The Alabama Data Breach Notification Act of 2018*, 79 ALA. LAW. 333, 334 (2018) (discussing the Alabama Breach Notification Act).

suit by the attorney general. Offering too little information also alienates data breach victims, who may perceive the lack of transparency as a disregard for their privacy and minimization of the seriousness of the situation. This could result in more reputational harm than necessary and subsequent customer churning. More information makes the entity appear more transparent and assures the customer that the entity is concerned with handling the situation, which may help avoid customer churning.

Detailed notifications also benefit consumers. After all, the purpose of breach notification is to empower data breach victims to take remedial action to avoid becoming victims of fraud.[192] Notifications that do not specify what data was compromised do little to assist consumers. Consumers remain unaware of what accounts they need to monitor, what cards they need to cancel, or what passwords they need to change. In addition, the ITRC recently launched a new remediation tool, giving consumers case-by-case assistance post-breach.[193] Vague notifications detract from the effectiveness of the remediation tool—the ITRC "cannot provide the affected consumers the action plans they need and deserve because [ITRC] cannot assess what their true risk is."[194] To ensure that Kansas consumers receive the best possible assistance with the new remediation tool, it is necessary to prescribe the substance of notification.

Beyond the substance of the notification, Kansas should modify the form of notice. Notification requirements should follow a structured notification system, with higher notification requirements for more sensitive data. For example, if the data exposed includes names and social security numbers, the data breach victim is at an extremely high risk for identity theft and the business should notify the victim strictly by post or phone. Substitute notice should be unavailable in these situations. For data breaches involving less sensitive data—such as name, date of birth, and credit card number—notice may be provided through email or substitute notice (in accordance with the current requirements).

Businesses would benefit from a hierarchy of notification requirements because direct contact is better-received by aggrieved consumers. A 2005 Ponemon survey showed that entities were three times less likely to lose business if notification was given via phone call or mailed letter, as opposed to email notification.[195]

---

192. ABLON, ET AL., *supra* note 125, at 2–3.

193. 2018 END-OF-YEAR DATA BREACH REPORT, *supra* note 11, at 4.

194. *Id.* at 5.

195. Although this study is dated, it is fair to assume that consumers still value direct contact over indirect contact, such as emails. PONEMON INST, NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 2 (2005), https://dl.packetstormsecurity.net/papers/general/Security_Breach_Survey.pdf [https://perma.cc/9Y4G-G9KY].

IV. CONCLUSION

In the absence of federal regulation, states have taken a greater role in regulating businesses that gather, maintain, and use consumer information. Data breach notification statutes are often the primary deterrent—through the threat of reputational harm—of negligent data security practices and the primary incentive for businesses to invest more in data security. Data breach notification statutes are necessary for consumers to mitigate their risk of identity theft or fraudulent charges. These statutes, however, are only effective if strong and clear. The current Kansas data breach notification laws are lax and should be strengthened to expand the definition of "personal information," include a hard deadline by which affected individuals must be notified, require notification to the attorney general to assist in identifying data breach trends, and include guidelines on the form and substance of notification.

Other states have reacted strongly to the Equifax breach and are taking data security more seriously than ever. Kansas should keep stride with other states and impose stronger breach notification requirements to protect Kansas consumers and improve the general data security infrastructure of Kansas businesses. Failure to do so could leave Kansas entities attractive targets to hackers, as other states make efforts to improve data security.