
# Data Breaches: Risk, Recovery, and Regulation

Alex Rosenberg
legislative analyst

WISCONSIN POLICY PROJECT • May 2019, Volume 2, Number 4

One East Main Street, Suite 200, Madison, Wisconsin 53703
http://legis.wisconsin.gov/lrb • 608-504-5801

## Introduction

Companies such as Adobe, Comcast, Dropbox, Imgur, Kickstarter, LinkedIn, MyFitnessPal, Snapchat, and Tumblr are all Internet mainstays with tens to hundreds of millions of users. It is likely that any given consumer in the United States has an account or otherwise regularly interacts with many, or even all, of these companies' services. Because each of these companies has had a major data breach in the past five years, it is also likely that for any given U.S. consumer, one or more of these incidents have exposed sensitive personal or financial data.

Even for savvy and mindful consumers, it can be difficult to keep track of what information they share and with whom. Consumers are not always aware of how much data a company has on them in the first place, let alone what data might be exposed in a breach. Often, consumers discover an issue only when they have already become the victims of identity theft or credit card fraud. Recovery, if it is possible, is both expensive and time consuming.

This report provides information to help inform state legislative efforts to protect consumers from the effects of data breaches. First, the report examines several tech and security industry studies to summarize the essential questions of data breaches. Next, the report briefly describes the added threats and policy implications of unknown or undisclosed breaches, specifically by firms whose business models rely on data collection. Finally, the report presents examples of breach-related legislation across the states, as well as major case law on the subject. Additionally, the appendix includes information to help prevent and recover from breaches.

## What is a breach?

A breach, according to Verizon Enterprise's Data Breach Investigations Report, is "an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party," and might take a number of forms:[1]

**Mistakes**—For example, hitting "reply all" rather than "reply" might lead to a sensitive email going far beyond the intended recipient.

**Physical security flaws**—An unlocked door or a lost USB drive could allow access to privileged records, for example.

**Social engineering**—"Phishing" scams, for example, trick a victim into giving up information to a fake version of a trustworthy person or site.[2]

1. Verizon Enterprise, *2018 Data Breach Investigations Report*, 2018, https://enterprise.verizon.com. The report aggregates and analyzes breach data that have been either investigated directly by Verizon Enterprise (Verizon Enterprise is the business-to-business service division of Verizon Communications) or provided by one of the contributing organizations Verizon lists in Appendix I (p. 66).

2. See the Department of Agriculture, Trade, and Consumer Protection's helpful page on phishing for more details and

**Hacking**—An attacker might gain illicit access to a website by exploiting a flaw in its log-in page, for example, which allows him or her to harvest data from the site.

Not all cases of compromised data security are breaches; data can be exposed but not taken advantage of. For example, an open filing cabinet drawer exposes files, but exposure does not guarantee that someone steals them. The Verizon report calls these cases "incidents," meaning "a security event that compromises the integrity, confidentiality or availability of an information asset."[3]

## Why steal data?

Those perpetrating or profiting from breaches are not necessarily interested in disclosing their motives, so information on why they do what they do can be scarce. However, Verizon Enterprise's study does claim to have found the following approximate frequency distribution of potential motives for breaches:[4]

**Financial: 60–80 percent.** Most breaches are motivated by profit obtained through direct theft of financial or payment data or by stealing other data that can be used for identity theft or sold to others looking to profit from it.

**Espionage: 10–30 percent.** Attackers can use data breaches to steal secrets, most commonly in the education (e.g., university research), manufacturing (e.g., industrial designs), and public (e.g., state secrets) sectors.

**Fun: 5–10 percent.** Curiosity can motivate breaches such as attempts to look up a celebrity's medical records or grades in school.

**Grudge: 1–5 percent.** Some data breaches have no particular benefit for the perpetrator, but are instead motivated by anger, jealousy, or distaste.

## What data is stolen in breaches?

The types of data stolen depend largely on the target; certain organizations have certain types of valuable data. The table below summarizes the Verizon Enterprise study's findings of nine industry sectors' most frequently stolen data types.[5]

Notably, the personal data category is among the top-three categories across every industry; additionally, personal data is the top category in five of the nine industries and represents about 42 percent of all breaches in 2018.[6] In many states' statutes (including Wisconsin's), this data is generally referred to as **"Personally identifiable information"**

---

recommendations to avoid falling victim to phishing and related schemes.

3. *2018 Data Breach Investigations Report*, p. 2.

4. Id. The methodology behind these data is not disclosed.

5. Id., pp. 4–5. Categories may overlap, as many breaches steal more than one type of data.

6. *2018 Data Breach Investigations Report*, p. 4.

**(PII)**: data that could be used to identify, find, or impersonate a specific person. In the absence of an overarching federal privacy regulation, statutory definitions of PII vary by application and jurisdiction. For example, section 943.201 of the Wisconsin Statutes lists examples of PII, including identifying documents, names, addresses, phone numbers, ID and account numbers, employer information, and DNA information. Statutes in other states might include different items in their definitions.

Table 1. **Industries' top three categories of data stolen in breaches.**

| | Education | Finance | Health | Hospitality | IT | Manufacturing | Services | Gov't | Retail |
|---|---|---|---|---|---|---|---|---|---|
| **1st** | Personal (72%) | Personal (36%) | Medical (79%) | Payment (93%) | Personal (56%) | Personal (32%) | Personal (56%) | Personal (41%) | Payment (73%) |
| **2nd** | Research/ secrets (14%) | Payment (34%) | Personal (37%) | Personal (5%) | Login/ security (41%) | Research/ secrets (30%) | Login/ security (28%) | Research/ secrets (24%) | Personal (16%) |
| **3rd** | Medical (11%) | Banking (13%) | Payment (4%) | Login/ security (2%) | Research/ secrets (9%) | Login/ security (24%) | Research/ secrets (16%) | Medical (14%) | Login/ security (8%) |

## Where do breaches happen?

Breaches happen everywhere, but findings from studies on the industries most affected by breaches can vary significantly. Table 2 compiles four major studies' top rankings of the industries most affected.

Table 2. **Four studies' rankings of industries affected by data breaches.**

| | IBM/Ponemon[7] | Identity Theft Resource Center[8] | Trend Micro[9] | Verizon Enterprise[10] |
|---|---|---|---|---|
| **1st** | Tech & service* (28%) | Business (55%) | Healthcare (27%) | Healthcare (28%) |
| **2nd** | Finance (16%) | Healthcare (24%) | Education (17%) | Hospitality (18%) |
| **3rd** | Manufacturing (14%) | Finance* (9%) | Public sector (16%) | Public sector (16%) |
| **4th** | Retail (7%) | Education (8%) | Finance† (14%) | Tech & service* (13%) |
| **5th** | Public sector (7%) | Public sector* (5%) | Retail (13%) | Retail (9%) |
| **6th** | Consumer (5%) | — | Tech & service* (6%) | Finance (8%) |

* Categories added together from the original report in order to improve consistency across the rankings.

7. Ponemon Institute and IBM, *2018 Cost of a Data Breach Study: Global Overview*, July 2018, https://www.ibm.com, p. 14. The Ponemon Institute is an independent data security research firm.

8. Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review Executive Summary*, January 2018, https://idtheftcenter.org.

9. Numaan Huq, *Follow the Data: Analyzing Breaches by Industry*, Trend Micro, 2015, https://www.trendmicro.com.

10. *2018 Data Breach Investigations Report—Executive Summary*, p. 4.

Given the variability among the studies, it is difficult to draw a clear conclusion about patterns in the targets of breaches. Each of the studies examined hundreds or thousands of breaches, and each found varied but high numbers of breaches across half a dozen or more industries. The safest conclusion, therefore, might be that while healthcare and tech breaches are somewhat more common, every industry has valuable data that can be stolen, so every industry is a target.

## When do breaches occur?

Breaches happen constantly. A 2018 IBM/Ponemon Institute study found that in the next 24 months, the average probability of a significant breach at any given organization is 27.9 percent.[11] This translates to a very large number records exposed and lost due to breaches every year. For example, in 2017, the Identity Theft Resource Center tracked 1,579 data breaches exposing 178,955,069 records—an average of more than six breaches and 490,000 records exposed per day. Verizon Enterprise's most recent annual study tracked 2,216 breaches with confirmed data theft, as well as 53,000 additional incidents that may or may not have led to data theft—an average of over six breaches and nearly 150 incidents per day over the course of the year.

Studies confirm that breaches happen far faster than we can respond to them. Verizon Enterprise, for example, breaks down the stages of a breach and time elapsed as a breach is carried out, found, and fixed:[12]

1. **Compromise (seconds to minutes)**: time spent breaking into a system.
2. **Exfiltration (minutes to hours)**: time spent getting data out of the system.
3. **Discovery (months)**: time taken to identify that a breach took place.
4. **Containment (minutes to weeks)**: time taken to close the vulnerability.

The Verizon Enterprise data show that the time it takes to discover and contain a breach can be much longer than the time it takes to break into a system and extract its data. The IBM/Ponemon study shows similar results. While the study did not track compromise or exfiltration, it shows an average discovery time of 197 days and an average containment time of 69 days post-discovery.[13] Together, those numbers add up to an average of nearly nine months of uncontained access in a breach. Some real-world breaches far exceed these averages; for example, in November 2018, Marriott disclosed a breach of over 500 million records that had been ongoing since 2014.[14]

---

11. *2018 Cost of a Data Breach Study: Global Overview*, p. 3. "Significant" here means over 1,000 records lost.

12. *2018 Data Breach Investigations Report*, p. 10.

13. *2018 Cost of a Data Breach Study: Global Overview*, p. 9.

14. Taylor Telford and Craig Timberg, "Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests," *Washington Post*, November 30, 2018, https://www.washingtonpost.com/.

Lengthy periods of vulnerability allow for a lot of damage to be done, contributing to an average cost of $148 per record stolen in a U.S. data breach.[15] For a business in the United States, the average total cost of a single breach is $7.91 million.[16] Costs to the consumers whose data are stolen are harder to measure, but one study suggests that identity fraud cost U.S. consumers nearly $17 billion in 2017.[17]

## How is a breach perpetrated?

There is some disagreement over the most common root causes of data breaches. Several studies, for example, find that human error causes 52 to 85 percent of breaches, making it by far the most common cause.[18] Other research finds lower percentages for human error as compared to other causes. The IBM/Ponemon cybersecurity study, for example, claims that only 27 percent of breaches are caused by human error, while 48 percent stem from "malicious or criminal attack."[19]

Whether or not it is the most prevalent cause, human error is undoubtedly a major source of breaches. Possible errors could include sending an email to the wrong address, misplacing physical media such as paper records or data drives, or simply leaving information in an unsecured location.

Breaches not caused by human error almost always stem from one of two other causes: technical glitches or malicious attacks. Technical glitches can be similar to human errors; for example, glitches might also lead to misdirected email, misplaced data, or holes in security.

Malicious attacks aim to create or take advantage of either human errors or technical glitches. For example, a phishing scheme takes advantage of human error by tricking a message recipient into sharing privileged information. Other attacks such as hacking, malware, and point-of-sale attacks take advantage of glitches or other technical vulnerabilities in order to access a system and steal data. Better training and security practices can repel attacks, but in practical terms, human error and glitches cannot be eliminated, so some attacks will inevitably succeed.

## How do breached organizations recover?

Cybersecurity professionals watch for and respond to cyberattacks and breaches in a

15. *Security Intelligence* (blog), "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT," by Larry Ponemon, posted July 11, 2018, https://securityintelligence.com.

16. 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/.

17. Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime*, 2018, https://www.iii.org.

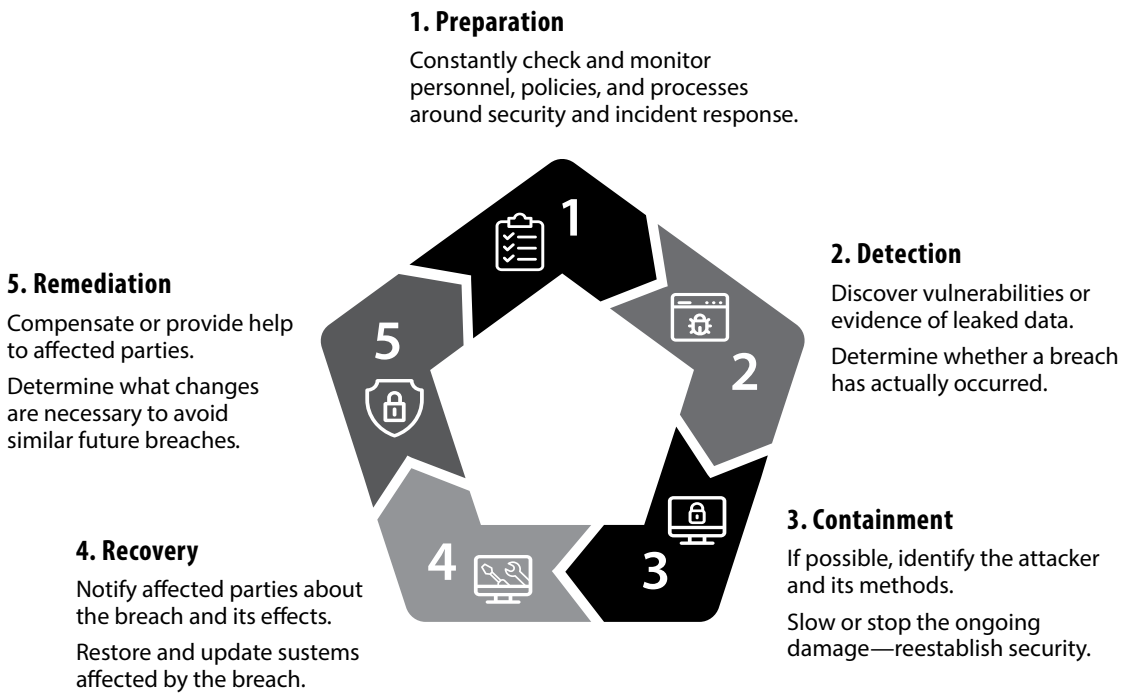
18. Computing Technology Industry Association (CompTIA), *Cybersecurity for Everyone, Not Just the IT Department*, 2016, https://www.comptia.org; Mahmoud Sher-Jan, "Data Indicates Human Error Prevailing Cause of Breaches, Incidents," *International Association of Privacy Professionals*, June 26, 2018, https://iapp.org; Phil Muncaster, "ICO Breach Reports Jump 75% as Human Error Dominates," *Infosecurity Magazine*, September 4, 2018, https://www.infosecurity-magazine.com.

19. *2018 Cost of a Data Breach Study: Global Overview*, p. 19.

constant, cyclical pattern. While organizations' approaches to data security vary, the process of preparing for, handling, and recovering from breaches follows this overall cycle:[20]

1. **Preparation:** taking measures to prevent breaches, but preparing for any that occur.
2. **Detection:** identifying breaches as or after they occur.
3. **Containment:** stopping the ongoing theft of exposed data.
4. **Recovery:** fixing damage and preventing future repetition of past breaches.
5. **Remediation:** helping victims of past breaches and returning to preparation for the future.

Figure 1**. The cyclical process of preparing for and dealing with data breaches.**




## Who perpetrates or takes advantage of data breaches?

Not all breaches come from the outside; internal actors can be as much or more of a risk as external ones. For example, internal breaches might take place when an employee leaks privileged secrets or sells access to information that could help a malicious actor bypass security measures. Verizon Enterprise's most recent study found that 28 percent of

20. Adapted from guidance and incident plans including Paul Cichonski et al., *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, August 2012, https://www.nist.gov; Carnegie Mellon University Information Security Office, *Incident Response Plan*, February 23, 2015, https://www.cmu.edu; Kent State University *Information Services, Information Security Incident Response Plan*, October 26, 2018, https://www.kent.edu.

all breaches involved internal actors.[21] Internal breaches are most common in industries with particularly valuable or interesting insider information. For example, 56 percent of healthcare breaches came from internal actors. Governments (34 percent) and professional service firms (31 percent) were also more likely than average to suffer breaches from internal actors.[22] The manufacturing (13 percent), retail (10 percent), and hospitality (1 percent) industries are relatively less affected by internal threats.

Most external breaches come from organized groups, not individuals. Organized criminal groups carried out 50 percent of breaches and state-affiliated actors carried out another 12 percent.[23] Various other individuals or groups, neither internal to the breached organization nor affiliated with organized crime or a nation-state, carried out the last 10 percent of breaches.

## Example breaches

Here are a few of the largest data breaches that took place in 2018:

- Facebook exposed at least 87 million profile records, including demographic, personality, social, and site/app engagement information.[24]
- Fitness and nutrition site MyFitnessPal exposed 150 million user records including usernames, email addresses, and encrypted passwords.[25]
- Saks Fifth Avenue and Lord & Taylor exposed more than 5 million payment cards.[26]
- UnityPoint Health exposed 1.4 million patients' demographic, medical, and insurance information, and possibly payment card and social security information as well.[27]

Even purportedly security-savvy organizations are not immune: identity theft protection firm LifeLock exposed 4.5 million users' email addresses in a way that also allowed bad actors to unsubscribe those users from LifeLock communications (such as email that could warn them about data security issues).[28]

Table 3 describes two hypothetical breaches across the five stages of the breach-fix cycle: a low-tech filing cabinet breach and a high-tech database breach.

---

21. *2018 Data Breach Investigations Report*, p. 5.

22. Verizon Enterprise, *2018 Data Breach Investigations Report Executive Summary*, 2018, pp. 4–5, https://enterprise.verizon.com.

23. Id.

24. Bill Hutchinson, "87 Million Facebook Users to Find out If Their Personal Data Was Breached," ABC News, April 9, 2018, https://www.abcnews.com.

25. Tony Bradley, "Security Experts Weigh In On Massive Data Breach Of 150 Million MyFitnessPal Accounts," *Forbes*, March 30, 2018, https://www.forbes.com.

26. Robert McMillan and Suzanne Kapner, "Saks, Lord & Taylor Hit With Data Breach," *Wall Street Journal*, April 2, 2018, sec. Tech, https://www.wsj.com.

27. David Wahlberg, "Second Data Breach at UnityPoint Health Added to Class Action Lawsuit," *Wisconsin State Journal*, August 14, 2018, https://madison.com.

28. Krebs on Security (blog), "LifeLock Bug Exposed Millions of Customer Email Addresses," by Brian Krebs, July 18, 2018, https://krebsonsecurity.com.

Table 3. **Two example data-breach scenarios.**

| Stage | Low-tech (filing cabinet) | High-tech (secure database) |
|---|---|---|
| **Preparation** | • We buy only filing cabinets with locking drawers.<br>• Keys are issued to trusted administrative staff.<br>• Staff are instructed to lock any drawer not in use. | • We buy modern, secure servers and protective software.<br>• Only administrators have access to the data server.<br>• Security and file backup procedures are in place. |
| **Detection** | • We notice a drawer is ajar and unattended.<br>• Several file folders have been refiled out of correct filing order (evidence of leaked data).<br>• We suspect someone unauthorized used them. | • A security audit shows a database access from an unknown user.<br>• Investigation shows a bug in our login page that may have been exploited (vulnerability).<br>• We have to assume a breach. |
| **Containment** | • We move the filing cabinet to a locked storage room to prevent any further access.<br>• We survey staff to figure out who might have gotten into the files.<br>• Nobody admits fault. | • We disconnect the compromised server from the network.<br>• We attempt to trace the network path of the unknown user.<br>• We hit a dead end at an offshore anonymous server. |
| **Recovery** | • We notify the subjects of the files that their data was exposed.<br>• We buy a new filing cabinet that locks automatically.<br>• We check the contents and correctly refile the folders. | • We notify the subjects of the database that their data was exposed.<br>• We request a patch to fix the bug from the software vendor.<br>• We set up a new server from a known-good backup. |
| **Remediation** | • We offer identity protection services to affected customers.<br>• We revise policies that determine who gets keys to sensitive files.<br>• We set up a security camera in the room with the filing cabinets. | • We offer credit monitoring and identity protection services to affected customers.<br>• We revise procedures to audit access records more often.<br>• We hire a security firm to test for other vulnerabilities. |

## Additional risk from undiscovered and undisclosed breaches

Just as it can often take a long time for an organization to discover that it has been breached, there can be serious barriers to consumers learning when, where, and how their data has been exposed. First, in most cases, the consumer will not find out about the breach until the breached organization discovers it. An organization has to know about a breach before it can inform the affected consumers. A savvy consumer who regularly checks his or her credit report might notice an anomaly, but it would be essentially impossible to trace to its source to figure out when and where the breach took place, and what was taken. It then falls to breached organizations to disclose their breaches.

Breach disclosures are mandatory. As described in the section on breach-related legislation, all 50 states require breached organizations to notify affected individuals. However, the specifics of these requirements vary, and it can be difficult even for a well-intentioned organization to fulfill all of its responsibilities for notifications—particularly when dealing with consumers across multiple state jurisdictions. An organization without as much consideration for its customers might be particularly unlikely to provide effective notifications about breaches. This is the case in large part because statutory requirements for breach notifications offer little to no penalty for noncompliance. For example, Wisconsin's breach notification statute sets no explicit penalty for noncompliance, stating only in a subsection related to civil claims that "failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty" (Wis. Stat. § 134.98 (4)).

Usually, organizations are obligated to make reasonable attempts to contact individuals whose data has been breached, but those attempts are not always successful. A breached organization may not know the full identity or have correct, up-to-date contact information for each individual involved in the breach, for example. As a result, it often falls to individuals to figure out for themselves whether their own information might have been released. Sometimes this is simple—for example, the recent Marriott breach was widely publicized in the media, so anyone who recently stayed at a Marriott property most likely knows that he or she ought to be concerned. Other less-publicized breaches can make it more difficult for a consumer to keep up, and few of the thousands of breaches per year receive major media coverage.

A further complicating factor is that a consumer might not know whether a breached organization has any of his or her information. Organizations with which a consumer has never interacted can nevertheless hold significant amounts of the consumer's PII. For example, most consumers have probably never heard of CoreLogic, but the company maintains a real estate database that, it says, covers over 99 percent of both U.S. consumers and U.S. residential properties.[29]

CoreLogic and similar firms are often known as data brokers—companies whose business models revolve around aggregating and reselling consumer data to other businesses, which then use the data for customer profiling, marketing, background checks, and fraud detection. By and large, the whole process of data collection, sales, and usage takes place without consumers' knowledge. As a result, if a data broker were to be breached, a consumer might not notice at all, or might erroneously believe that because he or she has no personal business with the firm, none of his or her data could be exposed.

The more data a firm holds, the more valuable and damaging a breach can be. Therefore, because brokers collect so much data, they are prime targets. As one industry insider

29. CoreLogic, "Our Data," accessed September 24, 2018, https://www.corelogic.com.

summarized, "what more could you want if you wanted to gather intelligence . . . you'd want to see everything [consumers] do on the Web, everything they're buying. We've built this incredible machine that does that and we don't even realize it."[30] Data brokers, therefore, pose a double risk in terms of consumers' data: brokers are the perfect target for a breach, but brokers' breaches would also be among the most difficult for consumers to stay apprised of. "It's highly likely that one of these [data broker] companies have already been compromised," reports independent security researcher Samy Kamkar.[31] The process of resolving a breach might take some time after the breach occurs, and even then, many affected customers will remain unaware that their data has been exposed. These delays and complications might make regulatory reform on data brokers and breach-notification processes particularly valuable.

## Breach-related regulations and legislation

There is no overarching federal data breach protection or notification law. Instead, diverse and separate regulations cover individual areas of data privacy. The most prominent include the following:

- The Health Insurance Portability and Accountability Act (HIPAA) regulates medical information, the process of applying to healthcare providers, insurers, pharmacies, and more.
- The Fair Credit Reporting Act regulates the collection and disclosure of information such as credit history, credit capacity, character, and general reputation by consumer reporting agencies.
    - 2018 U.S. S. 2155 (became Federal Public Law 115-174) amends the Fair Credit Reporting Act (15 U.S.C. 1681c–1) to extend credit freezes from 90 days to one year in duration and requires that consumer reporting agencies freeze consumers' credit free of charge and in a timely manner.
- The Federal Trade Commission Act prohibits unfair or deceptive practices toward consumers, including online privacy and data security issues such as failures to comply with posted privacy policies and unauthorized disclosures of PII.
- The Financial Services Modernization Act regulates the use of consumers' financial information, including the disclosure of financial and related PII.

Federal legislation on data brokers has been introduced in multiple sessions but has not passed. For example, a version of the Data Broker Accountability and Transparency Act (DATA Act[32]) has been introduced in the 2013–14, 2015–16, and 2017–18 sessions.

30. Christopher Mims, "The Hacked Data Broker? Be Very Afraid," *Wall Street Journal*, September 8, 2015, https://www.wsj.com.

31. Mims, "The Hacked Data Broker? Be Very Afraid."

32. Not to be confused with the federal spending-related Digital Accountability and Transparency Act (DATA Act) of 2014, which passed.

In the absence of unified federal regulations, state-level consumer protections become all the more important. Examples of PII protections throughout the Wisconsin statutes are listed below:

- Section 16.61 (3) (u) directs the Public Records Board to create and maintain a registry of "records maintained by state agencies that contain personally identifiable information."
- Subchapter IV of chapter 19 sets requirements and restrictions on PII collection and disclosure by state authorities and employees.
- Section 115.297 (4) sets restrictions on retaining and sharing personally identifiable student and workforce data to the statewide student data system or for other research purposes.
- Section 134.98 requires timely notification about PII security breaches to those affected.
- Section 440.46 prohibits disclosure of passengers' PII by transportation companies.
- Section 943.201 prohibits the unauthorized use of PII to obtain money or property, to avoid civil or criminal processes or penalties, to harm a person or an estate, or to commit other similar acts.

Significant data breach–related legislation passed by other states in their most recent terms includes the following:

**Data security procedure enforcement.** California passed 2018 SB 1121, a data security law that, in part, provides for a private right of action in addition to enforcement of data-security requirements by the attorney general. The law also removes several requirements that might otherwise stand in the way of civil suits for data breaches.

Colorado passed particularly strict new consumer-data protections. Colorado HB18-1128 requires companies to "maintain reasonable security procedures" for the PII they collect, as well as to "maintain a written policy for the destruction and proper disposal of those documents." The bill also expands notification requirements for breaches.

If an organization has a cybersecurity program that meets certain requirements for protecting PII and other restricted information, Ohio 2018 SB 220 provides that organization with certain legal protections in the case of a data breach.

South Carolina 2018 H 4655 requires insurers and insurance brokers to develop and maintain comprehensive information security programs as a condition for licensure by the state Department of Insurance. These security programs must include administrative, technical, and physical safeguards for security and confidentiality of PII and other restricted information.

**Credit freezes.** Connecticut 2018 SB 472 prohibits consumer reporting agencies from charging a fee to consumers to place or remove security freezes, requires those agencies to notify other similar agencies of freeze-related requests, and lengthens the time frame during which certain breached businesses must offer identity theft protection

and mitigation services to customers. Similar bills to streamline or eliminate fees for credit freezes also passed in a number of other states.

In addition to streamlining processes related to credit freezes, Maryland 2018 HB 848 requires consumer reporting agencies to post a bond of up to $1 million to cover injuries to consumers from cybersecurity breaches, identity fraud, or violations of the bill's other provisions. The bill also increases the civil penalties for consumer reporting agencies' violations of regulations.

**Data brokers.** Vermont became the first state to impose major regulations on data brokers with 2018 H. 764. Under the new law, data brokers are required to register with the state attorney general, disclose their data privacy practices and any data breaches, and develop and maintain a comprehensive program of administrative, technical, and physical safeguards for data security.

**Security breach notifications.** All 50 states—as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands—now have legislation requiring organizations to notify individuals of security breaches involving PII. Most states require prompt notification, but often these "promptness" requirements tend to be vague and often do not set specific time limits. Some of the most common reforms across the states tighten these restrictions.

The National Conference of State Legislatures (NCSL) maintains a record of each state's regulations in this area. The NCSL analysis notes that "at least thirty-one states, Puerto Rico and D.C. in 2018 are considering measures that would amend existing security breach laws" to, for example, "expand the definition of 'personal information,' to set specific time frames within which a breach must be reported, or require reporting to the state's attorney general."[33]

Wisconsin's security breach notification statute is section 134.98, which has been in effect since 2006. Compared to other states, Wisconsin has a stricter-than-average notification window for breaches. Most states require only that notification takes place "without reasonable delay." Wisconsin is one of the nine states with the shortest time restriction, 45 days.

Despite the state's 45-day notification requirement, Wisconsin's data-breach laws are otherwise considered "less strict," according to an analysis by loss prevention company Digital Guardian.[34] On a strictness scale of 1–5, Digital Guardian rated Wisconsin a "2" along with eight other "less strict" states and U.S. territories—only two states had lower rankings. By contrast, 17 states or territories had a "3" rating, 14 had a "4," and 11 had a "5."[35] In the Digital Guardian analysis, "lower [strictness] ratings went to states that

33. National Conference of State Legislatures, "2018 Security Breach Legislation," October 12, 2018, http://www.ncsl.org.

34. Dan Lohrmann, "New Guide on State Data Breach Laws," *Government Technology*, September 1, 2018, http://www.govtech.com.

35. Id. In the study, Alaska was the only state with a split rating, which was marked as "4-5."

had longer notification deadlines, no or lesser penalties, fewer reporting requirements to state/credit reporting agencies, were more lax in terms of how residents are notified, or allowed substitute notification for a lower threshold (i.e., substitute notifications permitted if the cost exceeds $10,000 or more than 500 residents must be notified vs. when the cost exceeds $250,000 or more than 50,000 residents must be notified)."[36]

## Breach-related case law

***Clapper v. Amnesty International USA***[37]—While not about data breaches, this case sets much of the foundation for ongoing breach-related legal conflicts. Plaintiffs in the original case sought to challenge the constitutionality of Foreign Intelligence Surveillance Act (FISA) surveillance. The case reached the Supreme Court after a federal court ruled that the plaintiffs had not shown that they would be targeted, but the court of appeals subsequently ruled that the likelihood of the plaintiffs being surveilled was enough for them to have standing to sue.[38] Ultimately, the Supreme Court held that reasonable likelihood of surveillance did not suffice to show future injury, and so was not sufficient for standing. Similarly, costly measures taken to avoid surveillance also did not constitute an injury.

Questions about standing relating to speculative future harm and costly measures taken to mitigate that future harm go on to be core elements of many data breach–related cases over subsequent years.

***Spokeo, Inc. v. Robins***[39]—Thomas Robins filed a class action suit against "people search engine" Spokeo regarding inaccurate information about him on the site, alleging that Spokeo willfully violated the Fair Credit Reporting Act requirement to "follow reasonable procedures to assure maximum possible accuracy" of consumer reports (15 U.S.C. § 1681e(b)). The district court dismissed Robins's suit because he had not demonstrated clear personal injury, but the Ninth Circuit Court reversed this decision, holding that violation of Robins's statutory rights and "personal interests in the handling of his credit information" were individualized harms.[40] The Supreme Court vacated and remanded the ruling, holding that the Ninth Circuit Court had failed to consider both aspects of the injury-in-fact requirement, identifying harms to Robins but not determining the concreteness of those harms. The Supreme Court did not take a position on "whether the Ninth Circuit's ultimate conclusion—that Robins adequately alleged an injury in fact—was correct."

---

36. Id.

37. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 133 S. Ct. 1138 (2013).

38. Amnesty Int'l United States v. McConnell, 646 F. Supp. 2d 633 (S.D.N.Y. 2009); Amnesty Int'l United States v. Clapper, 638 F.3d 118 (2d Cir. 2011).

39. Spokeo, Inc. v Robins, 13-1339 (2016).

40. Robins v. Spokeo, Inc., 742 F.3d 409 (9th Cir. 2014).

In August 2017 the Ninth Circuit held that Robins had alleged a concrete harm, and therefore established an injury in fact.[41] Spokeo filed a petition for a writ of certiorari in the Supreme Court following this Ninth Circuit decision, but the Supreme Court denied the petition in January 2018.

Without decisive Supreme Court precedent on the issue, *Spokeo* can be cited as precedent for future cases that rely on the risk of future harm from data breaches to establish standing. See, for example, *Macy v. GC Servs. Ltd. P'ship*, 897 F.3d 747 (6th Cir. 2018). However, cases since *Spokeo* show a "significant circuit court split as to whether an increased risk of future harm is sufficient to support Article III standing," suggesting that the issue may remain unclear until potential future Supreme Court action.[42]

***CareFirst v. Attias***[43]—Members with health insurance from CareFirst, Inc., filed a class action suit against CareFirst after the company was hacked in 2014, alleging that the stolen personal information from CareFirst's servers put them at risk for identity theft in the future. The U.S. District Court for the District of Columbia dismissed the suit, holding that "merely having one's personal information stolen in a data breach is insufficient to establish standing."[44] The D.C. court of appeals reversed the circuit court decision, holding that unauthorized access to PII—even if the PII does not include social security numbers or credit card numbers—does in fact create a sufficient risk of identity theft to establish standing.[45]

CareFirst filed a petition for a writ of certiorari, but the Supreme Court denied the petition, therefore permitting the class action suit to proceed. Once again, this leaves the question of injury standing for data breaches unresolved at the level of the Supreme Court. As a result, individual lower courts will have to confer or deny standing in the absence of guidance for measuring the risks and concreteness of harms that stem from data breaches and similar issues.

***Carpenter v. United States***[46]—Following a conviction for a series of armed robberies, Timothy Carpenter challenged the admissibility of cell phone–location records that were used as part of the case against him. Both the district court and the court of appeals found in favor of the government, upholding the permissibility of using the cell phone records.[47] The Supreme Court reversed and remanded the earlier ruling, holding that the government's acquisition and use of the cell phone records was a search under the

41. Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).

42. Dominic Spinelli, "Data Breach Standing: Recent Decisions Show Growing Circuit Court Split," *American Bar Association*, January 18, 2019, https://www.americanbar.org.

43. CareFirst, Inc. v. Attias, 138 S. Ct. 981 (2018).

44. Attias v. CareFirst, Inc., 199 F. Supp. 3d 193 (D.D.C. 2016).

45. Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).

46. Carpenter v. United States, 138 S. Ct. 2206 (2018).

47. United States v. Carpenter, No. 12-20218, 2013 U.S. Dist. LEXIS 172508 (E.D. Mich. Dec. 6, 2013); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016).

Fourth Amendment, and so was an unreasonable invasion of privacy in the absence of a warrant.[48]

Despite Chief Justice Roberts's argument in the court's decision that it is "a narrow one," there is speculation in the legal community that the logic behind the court finding a legitimate privacy interest in cell phone–location records might also be applied to other areas of digital privacy and have significant impact on Fourth Amendment jurisprudence in the future.[49]

## Conclusion

Data breaches continue to grow in both prevalence and impact, while a clear and comprehensive regulatory strategy to deal with them has not yet emerged. Attackers' continued exploration of new and unanticipated avenues for data theft are also testing the boundaries of existing consumer privacy protection regulations, where holes in regulation or areas of confusion might emerge only after an incident has taken place. Because of the diversity of federal consumer protection regulations and the lack of a single overarching privacy rule, state-level action can be an effective method to fill in regulatory holes and deliver targeted relief to constituents in the wake of a breach.

As data breaches remain in the news and are likely to affect many constituents of any legislator, there will likely continue to be significant demand for regulatory action to combat these cyber threats. Breaches will continue to spread and evolve, and so too must the regulations that can protect consumers from their effects. ■

48. Carpenter v. United States, 138 S. Ct. 2206 (2018).

49. Susan Freiwald and Stephen Wm Smith, "The Carpenter Chronicle: A Near-Perfect Surveillance," *Harvard Law Review* 132 (November 9, 2018): 227–31, https://harvardlawreview.org; "SCOTUS Issues Landmark Decision on Cell Phone Location Data with Major Implications for Fourth Amendment Privacy," *The National Law Review*, accessed March 5, 2019, https://www.natlawreview.com.

## Appendix: How to personally avoid and recover from data breaches

### Best practices to help eliminate risk from breaches

When so many companies hold so much of our data, it can feel difficult or impossible to have any individual control over breaches of one's own information. However, there are several simple behaviors that can help individuals to avoid or lessen the impacts of data breaches:

- **Use unique passwords.** Using the same or very similar passwords across multiple accounts can mean that a breach of any one of them exposes your information across all accounts. Using unique usernames and passwords for each sensitive account can help ensure that the effects of any individual breach remain as confined as possible.
- **Use a password manager.** Practically speaking, it can be impossible to use and remember unique passwords across dozens or even hundreds of online accounts. Password managers exist to solve this problem. The user only has to remember and enter a single secure "master password," while the password manager can generate, store, and automatically fill in secure login information for all of the user's accounts. Leading password managers include LastPass, Dashlane, and KeePass.
- **Use two-factor authentication.** Two-factor authentication (2FA) requires something else in addition to a password before granting access to an account. Most often, this second "factor" is a randomly generated, short-term code that only the rightful account holder should be able to access. For example, logging into an online bank account might require the user to enter both a password and a code sent to the cell number registered with the account. Apps, physical hardware, and biometrics such as fingerprints can also be used for 2FA; Google Authenticator is probably the most widely used solution.
- **Limit data sharing.** Individuals should take care before disclosing sensitive data, as limiting the data that one shares online can reduce the potential for exposure in a breach. When a site offers to store credit card data for future transactions, for example, declining the offer can help to keep the card safe from future breaches. Deleting unused apps and scaling back social media account access to smartphone functions such as contact lists and location services can also be helpful ways to limit data exposure.

### Best practices for individual breach victims

Upon receiving notification or otherwise discovering that one has been a victim of a breach, authorities including the U.S. Federal Trade Commission and the Wisconsin Department of Agriculture, Trade and Consumer Protection recommend the following course of action:[50]

50. See, e.g., "Consumer Protection Fact Sheet—ID Theft Steps for Data Breaches," Wisconsin Department of Agriculture, Trade and Consumer Protection, September 2018, https://datcp.wi.gov; "Identity Theft Recovery Steps," IdentityTheft.gov:

1. If possible, determine what data have been stolen, and use that information to guide further steps. For example, stolen payment card information points toward fraudulent charges, while a stolen social security number might point toward identity theft.
2. Contact affected companies and ask to close or freeze accounts. Change any login information, passwords, PINs, or other security measures in place for those accounts.
3. Place a fraud alert with any of the three credit reporting agencies (Experian, Equifax, or TransUnion). The fraud alert adds a flag to the agencies' credit files to indicate the potential for fraud or identity theft and the need for extra identity verification. The request to any one of the three agencies will also alert the other two. Fraud alerts are free and remain in effect for one year; they can be extended as needed in cases of confirmed identity theft.
4. Report identity theft to the police department. A police report regarding identity theft can be used as evidence in banks' and credit card companies' fraud-recovery processes.
5. Monitor credit reports and other accounts for issues. Often, breached businesses offer free credit protection services that can help with this monitoring. If fraudulent charges, inaccurate account activity, or other issues appear, notify the affected business immediately. Continue to monitor these accounts for future issues.

Federal Trade Commission, accessed January 29, 2019, https://identitytheft.gov/Steps.