Avoiding the Siren Call of the Clock in "Unreasonable Delay" Data Breach Notification Cases

Evan Yahng

Avoiding the Siren Call of the Clock in "Unreasonable Delay" Data Breach Notification Cases

*Evan Yahng**

As online personally identifiable information, data breaches, blockchain, Artificial Intelligence, and other trends in the cyber ecosystem proliferate, courts must confront legal questions about data privacy that past courts have kicked down the road. One such question that courts and scholars have yet to properly interrogate is what constitutes "unreasonable delay" in violation of state data breach notification statutes.

All fifty states, the District of Columbia, Puerto Rico, the Virgin Islands, and Guam have laws requiring companies that hold data to provide notice to data subjects in the event such data is compromised. But courts have been able to punt the question of delay until now because data breach litigation often dies early, either because the statute does not provide a cause of action, or because the harm is too speculative to support a cause of action in negligence. With courts recognizing more statutory causes of action and more harms in negligence, the time to answer the question has come. Indeed, a massive number of courts addressed unreasonably delayed data breach notice claims in 2024.

A substantial number of those courts made a grave error when they denied motions to dismiss solely because precedent in their jurisdictions held that a given number of days was prima facie unreasonable. This Article argues that this approach misunderstands the purpose of data breach notification laws and leads to undesirable results including costly liability for companies and risks to individual consumers' identities. After sampling some of these 2024 cases, this Article explains myriad problems associated with relying on the clock as the sole indicator of reasonableness. Finally, this Article suggests that courts follow a more practical and doctrinally desirable approach whereby they examine defendants' post-breach investigation to determine whether any delay was unreasonable.

---

* J.D., Washington University in St. Louis; B.A., Xavier University. The author is a private attorney. Any and all views and opinions expressed herein belong solely to the author and do not necessarily reflect the views of the author's employer.

I. INTRODUCTION

Everyone has had a data breach notification letter appear in their mailbox, but who is to blame when it comes too late? Your credit card has already been used, a bank account has already been opened in your name, and your inbox has already been filled with spam. Courts across the country have recently confronted whether a defendant's delay in sending notice of a data breach to the individuals whose information was exposed was "unreasonable" or not "as soon as possible" in violation of state law. A number of these courts denied motions to dismiss solely on the basis of precedent that a given number of days' delay was prima facie unreasonable.

This Article warns that relying on case law to determine whether a given number of days' delay is unreasonable misunderstands the purpose of data breach notification laws and leads to undesirable results. Courts should understand that whether a delay in sending breach notification is unreasonable is unripe to be resolved at the motion to dismiss stage. Courts must instead make case-by-case determinations in light of the totality of the circumstances at the motion for summary judgment stage or later. This requires interrogating the defendant's post-breach investigation, which may include retaining counsel, containing the breach, accurately determining the number and identity of victims, drafting the notice, and more. This approach is more thorough, beneficial to businesses and individuals, coherent in the long term, and consistent with the statutory purpose of data breach notification laws.

This Article proceeds in three parts. The first part samples some of the recent case law regarding whether delay in sending data breach notification is unreasonable. The second part explains the pitfalls of using the clock as the only indicator of reasonableness without interrogating the defendant's incident response, and why examining the facts of the post-breach investigation is practically and doctrinally more desirable for courts, litigants, affected individuals, and businesses. Finally, the third part considers the elements of a post-breach investigation that courts should examine when determining reasonableness. It should be noted that this Article focuses on whether a violation of a state data breach notification statute has occurred because the delay was unreasonable. This is separate from whether a delay was negligent, or whether it caused

cognizable injury or harm for standing, negligence, or other purposes. These questions have been well litigated (although courts have not reached a unanimous resolution) and are beyond the scope of this Article.

II. SUMMARY OF RECENT DELAY-OF-BREACH-NOTIFICATION CASES

2024 was a boom year for litigation of data breaches. Data breaches are an increasing problem for businesses and the millions of individuals whose data is in their hands.[1] Data incidents can result from criminal conduct such as hacking, insider theft, or phishing, as well as accidents such as mistaken publication or lost computers.[2] When unavoidable, a company can mitigate the effects of a data incident through actions including prompt containment, eradication, recovery, and notification to affected data subjects.[3] When mishandled, the costs of data incidents, both to businesses and data subjects, can be enormous. In 2024, the global average cost of a data breach was $4.88 million—a ten percent increase over the last year.[4] This problem is even worse in sectors like healthcare.[5] Individuals, meanwhile, may suffer the crippling financial and emotional consequences of identity theft that result from a data incident.

All fifty states, the District of Columbia, Puerto Rico, the Virgin Islands, and Guam have laws requiring companies that do business in their jurisdiction and that hold computerized data to provide notice to affected citizens in the event such data is compromised.[6] Depending on the risk of harm and the number of individuals or citizens affected, some of these laws also require

---

1 140 AM. JUR. *Trials* § 1 (2015); *see also* Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 J. ANTITRUST & UNFAIR COMPETITION L. 229, 229 (2015) ("Corporate legal spending on data security in the United States increased from $1 billion in 2013 to $1.4 billion in 2014, and is expected to climb to $1.5 billion in 2015—a 7.9% increase that dwarfs the next highest practice area (2.7% for class actions).").

2 140 AM. JUR. *Trials*, *supra* note 1, § 2.

3 *Id.*

4 *The Cost of Data Breaches*, THOMSON REUTERS (Dec. 11, 2024), https://legal.thomsonreuters.com/blog/the-cost-of-data-breaches/ [https://perma.cc/6VCP-Z3Z9].

5 140 AM. JUR. *Trials*, *supra* note 1, § 2 ("The study found the cost of these breaches to health care organizations in 2014 was significantly more expensive than in any other sector of the economy at $359 per capita in the health care sector compared to $206 in the financial services industry and $155 in consumer products organizations.").

6 David Garrison Golubock, *Remote Workers, Ever-Present Risk: Employer Liability for Data Breaches in the Era of Hybrid Workplaces*, 15 CASE W. RESERVE J.L. TECH. & INTERNET 305, 336 (2024).

notice to be given to a regulator and credit reporting agencies.[7] In all fifty states, the state attorney general may impose fines for violations, while approximately fifteen states also grant a private right of action to individuals harmed by the breach.[8] Many federal privacy statutes and regulations also require data breach notification and employ varying frameworks, though there is no general federal reporting law.[9]

While notice requirements vary by jurisdiction, companies must generally provide a description of the incident, including an approximate date; the types of data affected; the remedial steps the company has taken; and information regarding credit freezes, monitoring, and contact information for obtaining assistance from the Federal Trade Commission. While many states express a preference for notification by mail, states often permit alternative methods of notification such as telephone, email, or public posting under certain circumstances, including undue financial burden or insufficient consumer contact information.[10]

One of the main questions a company must answer when a data breach occurs is when to send notice. Some states require notification without unreasonable delay, subject to a specific maximum time limit. For example, Florida's statute reads:

> Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the

---

7 *See The Ultimate Guide to Data Breach Notification Laws by State*, EMBROKER (Feb. 28, 2025), https://www.embroker.com/blog/data-breach-laws-by-state/ [https://perma.cc/RPP8-DNMC].

8 *See id.*; *see also* PETER SWIRE AND DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 325 (4th ed. 2024) ("Nearly 15 states grant a private right of action to individuals harmed by disclosure of their personal information.").

9 *See* Golubock, *supra* note 6, at 337 (summarizing the existence or non-existence of a private right of action to enforce data breach notification requirements under the Health Insurance Portability and Accountability Act, Federal Communications Commission rules, Securities and Exchange Commission rules, Federal Trade Commission rules, Fair Credit Reporting Act, and Cyber Incident Reporting for Critical Infrastructure Act of 2022); Nicole B. Perkins, *Spreading a Digital Disease: The Circuit Split on Data Breaches and Its Effects on the Health Sector*, 20 IND. HEALTH L. REV. 435, 456 (2023) (discussing the Health Information Technology for Economic and Clinical Health Act's requirement that notification be provided without unreasonable delay and in no case later than sixty days following the discovery of a breach).

10 *See, e.g.*, CAL. CIV. CODE § 1798.82(j) (West 2025) (permitting written notice, electronic notice, or substitute notice if the cost of providing notice would exceed $250,000, the class of persons to be notified exceeds 500,000, or if the person or business does not have sufficient contact information).

> breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred . . . .[11]

The time limit may vary from thirty to ninety days, with an average of forty-five days,[12] though industry best practice for notification has converged on seventy-two hours due to the influence of the European Union's General Data Protection Regulation.[13] Other jurisdictions only require that notice is provided "without unreasonable delay" or "as soon as possible," without providing a defined time limit. For example, Arkansas' statute provides: "The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system."[14] This Article is principally concerned with statutes that follow the latter formulation.[15] While the question of when a delay is unreasonable can be relevant to statutes that set a specific number of days by which notification must be given,[16] there is less need for guidance (and the matter is less

---

11 FLA. STAT. § 501.171(4)(a) (2025); *see also* DEL. CODE ANN. tit. 6, § 12B-102(c) (2025) ("Notice . . . must be made without unreasonable delay but not later than 60 days after determination of the breach of security . . . ."); ALA. CODE § 8-38-5(b) (2025) ("Notice to individuals . . . shall be made as expeditiously as possible and without unreasonable delay . . . . [T]he covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third-party agent that a breach has occurred . . . .").

12 Carol M. Hayes, *Comparative Analysis of Data Breach Laws: Comprehension, Interpretation, and External Sources of Legislative Text*, 23 LEWIS & CLARK L. REV. 1221, 1260 (2020).

13 Scott J. Shackelford, Anne Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, 25 YALE J.L. & TECH. 86, 109–10 (2023).

14 ARK. CODE ANN. § 4-110-105(a)(2) (2025); *see also* GA. CODE ANN. § 10-1-912(a) (2025); ALASKA STAT. § 45.48.010 (2024); IOWA CODE § 715C.2 (2025); MONT. CODE ANN. § 2-6-1503(1)(a)–(b) (2025). Most statutes also permit delay if notification may impede a criminal investigation. *See, e.g.*, WYO. STAT. ANN. § 40-12-502(a)–(b) (2025) (providing both that notice shall be made "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system," and permitting notification to be "delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation").

15 The clock generally begins to run when a company "reasonably" believes, suspects, or confirms a data breach has occurred. When the clock starts ticking is separate from the reasonableness of the delay once the clock has started. *See* Hayes, *supra* note 12, at 1260–61.

16 For example, a court in Florida may need to determine whether a delay of less than thirty days was unreasonable or not as expeditiously as practicable. *See id.* at 1261.

likely to be disputed) when the legislature has established a specific timeline.[17]

Neither courts nor scholars have settled on what constitutes "unreasonable delay" in suits brought by individuals whose data was exposed.[18] This is due to the fact that data breach litigation often dies on the vine early, either because the statute does not provide a cause of action,[19] or because the harm is too speculative to support a cause of action in negligence.[20] But as data breaches continue to proliferate, breach-related lawsuits become more common, and as more courts recognize breach-related harms in negligence,[21] courts will have to address this issue. This Part highlights a sampling of the many data breach lawsuits from 2024 that measured the reasonableness of a delay by comparing it to timelines set by precedent. The sheer number of data breach cases that were brought in 2024 makes it impossible to summarize them all; therefore, this Article is not intended to be an exhaustive list.

A. California

Due to the number of Fortune 500 companies, data brokers, and other cyber-trailblazers in the state, California was unsurprisingly a hotbed for litigation of this issue in 2024. Under California's Customer Records Act (CRA), any person or entity that conducts business in California, and that owns or licenses computerized data containing personal information, must disclose a security breach of their system to all California residents whose unencrypted information (or encrypted information along with the key) was, or is reasonably believed to have been, acquired by an unauthorized person.[22] Notification

---

17 Also in Florida, after thirty days, this analysis would not be necessary. *See id.*

18 *See* Golubock, *supra* note 6 ("In theory, many of these laws do create a private right of action against businesses that fail to timely disclose a data breach. In practice, however, many of these statutes leave it up to courts to determine whether a business delayed unreasonably in notifying affected parties, and even delays of weeks may not be sufficient to support a claim for failure to notify.").

19 *See, e.g.*, N.Y. GEN. BUS. LAW § 899-aa (McKinney 2025); GA. CODE ANN. §§ 10-1-910 to -915 (West 2025).

20 *See, e.g.*, Mohsen v. Veridian Credit Union, 733 F. Supp. 3d 754, 763–65 (N.D. Iowa 2024) (holding that the economic loss rule barred a data breach-related negligence claim).

21 *See, e.g.*, Nunley v. Chelan-Douglas Health Dist., 558 P.3d 513, 517 (Wash. Ct. App. 2024) (holding that loss of time, mental distress, and loss of value of personal information satisfied Washington's common-law requirement that a plaintiff in a negligence case must prove damages).

22 CAL. CIV. CODE § 1798.82(a) (West 2025).

must be provided "in the most expedient time possible and without unreasonable delay," though no specific timeframe for disclosure is mandated.[23]

For example, in *Jackson v. Health Center Partners of Southern California*, the plaintiff alleged that the defendant's 139-day delay in disclosing a data breach violated the CRA.[24] Citing precedent, and without questioning the defendant's breach response, the court wrote:

> Some courts have found that five-month delays and nine-month delays in providing notice of a data breach sufficiently alleged an "unreasonable delay" under the CRA. In contrast, an alleged ten-day delay was not a sufficient allegation of unreasonable delay.
>
> . . . [A] court in a similar case alleging a violation of the CRA denied a motion to dismiss [and] . . . set for trial the CRA claim of a one-month delay . . . .
>
> . . . Today, Plaintiff's allegation of harm is sufficient, along with the allegation of unreasonable delay, to state a plausible state law cause of action under the CRA . . . .[25]

The court thus implicitly rejected the theory that the reasonableness of a particular delay under the CRA is a question for trial rather than for a motion to dismiss.[26]

The *Jackson* court cited *J.M. v. Illuminate Education, Inc.* for the proposition that a five-month delay was sufficient to survive a motion to dismiss.[27] There, the plaintiff alleged that the defendant, an education consultant, delayed disclosure of a breach for five months in violation of the CRA.[28] The California Court of Appeal held that a "five-month disclosure delay supports a cause of action under the CRA because such a delay prevents victims from taking prompt steps to protect their personal information."[29] Citing precedent regarding whether a plaintiff suffered injury, the court stated: "A delay of even three months in

---

23 *Id.*

24 Jackson v. Health Ctr. Partners of S. Cal., No. 24-cv-00106-BEN (DDL), 2024 WL 3708867, at *5 (S.D. Cal. Aug. 7, 2024).

25 *Id.* (citations omitted) (first citing J.M. v. Illuminate Educ., Inc., 323 Cal. Rptr. 3d 605, 612 (Cal. Ct. App. 2024); then citing *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014)).

26 *See id.* ("And at least one court has suggested that whether a particular delay qualifies as an 'unreasonable [delay] under' the CRA is normally a question for trial rather than for a motion to dismiss."). *Contra In re Sony*, 996 F. Supp. 2d at 1010.

27 *Jackson*, 2024 WL 3708867, at *5 (citing *J.M.*, 323 Cal. Rptr. 3d at 612).

28 *J.M.*, 323 Cal. Rptr. 3d at 609.

29 *Id.* at 613 (citation omitted).

notifying victims has been held to be sufficient to state a cause of action for damages under the CRA."[30]

B. Florida

On the other side of the country, the U.S. District Court for the Southern District of Florida addressed claims that a supplemental-benefits insurance provider's notice that the plaintiff's personal data was compromised under the CRA was unreasonably delayed.[31] Brushing past the issue, the court wrote: "Plaintiffs' allegation that Defendants failed to disclose the Data Breach 'in a timely and accurate fashion,' waiting until at least April 13, 2023, despite being notified by February 3, 2023, is similarly sufficient."[32] The court reasoned only that, at the pleading stage, it was bound to accept the plaintiffs' allegation that a two-month delay was unreasonable.[33]

C. New England

The Massachusetts District Court reached a similar holding when reviewing a putative subclass alleging a violation of New Hampshire's Notification of Security Breach Required law in its decision in *In re Shields Health Care Group, Inc. Data Breach Litigation*.[34] Plaintiffs, patients of a medical scanning and surgical services company whose data was compromised in a breach, alleged that the defendant took approximately four months to provide notification.[35] As a result, they claimed, they could not take measures to prevent injuries resulting from their information being for sale on the dark web, including fraudulent bank charges, suspicious email activity, emotional distress, and

30 *Id.* (citing *In re* Ambry Genetics Data Breach Litig., 567 F. Supp. 3d 1130, 1150 (C.D. Cal. 2021)).

31 *In re* Fortra File Transfer Software Data Sec. Breach Litig., No. 23-cv-60830-RAR, 2024 WL 4547212, at *14 (S.D. Fla. Sept. 18, 2024). The CRA claim was brought by a putative subclass comprised of California residents. *Id.* at *13.

32 *Id.* at *14 (citations omitted).

33 *Id.* It is not uncommon for courts to dedicate little ink to this issue. For example, in *Dusterhoft v. OneTouchPoint*, a Wisconsin case addressing claims under South Carolina's breach notification statute, the only attention the court gave the unreasonable delay issue was in the following sentences: "[The c]omplaint alleges that OneTouchPoint did not notify [plaintiff] of the breach until . . . a full three months after the breach occurred. This significant delay is sufficient to create a plausible inference that OneTouchPoint failed to notify [plaintiff] 'in the most expedient time possible,' as required by the statute." Dusterhoft v. OneTouchPoint Corp., No. 22-cv-0882-bhl, 2024 WL 4263762, at *20 (E.D. Wis. Sept. 23, 2024).

34 *In re* Shields Health Care Grp., Inc. Data Breach Litig., 721 F. Supp. 3d 152, 167–68 (quoting N.H. REV. STAT. ANN. § 359-C:20(I)(a) (2025)).

35 *Id.* at 158–59.

loss of value of the data.[36] The defendants moved to dismiss the New Hampshire breach notification claim, but the court denied the motion.[37]

New Hampshire's security breach law requires any person doing business in the state "who owns or licenses computerized data that includes personal information [to], when it becomes aware of a security breach, promptly determine" whether a misuse of the information has occurred or is reasonably likely to occur.[38] If the determination is made in the affirmative or if a determination cannot be made, the person must "notify the affected individuals as soon as possible."[39] The *Shields* subclass alleged the defendant's four-month delay was not "as soon as possible" as required by the statute.[40] The defendant rebutted that it immediately launched an investigation, and the complaint did not show that three months was an unreasonable investigation period.[41] The court compared New Hampshire's statute to other state laws that require companies to notify individuals of data breaches "without unreasonable delay," and concluded: "Courts interpreting statutes with similar language have not dismissed claims where the defendant waited nine months, five months, and four months to notify plaintiffs of a data breach. Thus, [plaintiff] has stated a claim under the New Hampshire notice statute."[42]

III. BLINDLY FOLLOWING CASE LAW REGARDING HOW MUCH TIME CONSTITUTES AN UNREASONABLE DELAY IS MISGUIDED

These 2024 cases relied on precedent as the end-all, be-all of what is or is not per se unreasonable for motion to dismiss purposes. In other words, the courts determined that if one hundred days had been held unreasonable in the past, then one hundred days must be prima facie unreasonable in the case before them. While this approach is not new, it is and always has been wrong. Using the clock alone is tempting and, at first glance, fits with how courts generally apply stare decisis. However, this approach misses what is actually going on. It is not that hours, days, or months themselves are unreasonable, but

36 *See id.* at 159.
37 *See id.* at 167–68.
38 N.H. REV. STAT. ANN. § 359-C:20(I)(a).
39 *Id.*
40 *In re Shields*, 721 F. Supp. 3d at 167.
41 *Id.*
42 *Id.* (citations omitted).

rather what caused the delay that may or may not be reasonable. Whether a data breach response is unreasonable cannot be divined by citations to other cases' timelines for three reasons: (1) it is unripe to be determined at the pleading stage, (2) it creates impractical results, and (3) it is inconsistent with the purpose of data breach statutes.

A. Whether a Delay in Sending a Data Breach Notice Is Unreasonable Is a Question of Fact to Be Determined at the Summary Judgment Stage or Later

That a data breach response was unreasonably delayed must, of course, be in the complaint. Therefore, courts can dismiss a case if the plaintiff fails to allege that a delay was unreasonable[43] or if there is a failure to allege a timeline from which it could be inferred that an unreasonable delay occurred[44] because a core element of the claim would be missing. But if a defendant moves to dismiss a properly alleged delay on the ground that the delay was not unreasonable, courts should refuse to decide the issue as unripe at that early stage. In data breach cases, as in most contexts, reasonableness itself is a question of fact for the factfinder to decide after weighing the evidence and credibility of witnesses.[45]

In individual cases, the practical result of either approach is the same: the motion to dismiss is denied. However, the "why" is important at the macro level. Data breaches are fact-intensive disputes that must address the number of individuals affected, the systems compromised, the method of exposure, the injuries the plaintiff suffered, and more. "Whether a delay was reasonable requires courts to look beyond the length of the delay and consider the facts alleged."[46] Inflexible, bright-line rules for

---

43 *See* Razuki v. Caliber Home Loans, Inc., No. 17-cv-1718-LAB (WVG), 2018 WL 6018361, at *2 (S.D. Cal. Nov. 15, 2018) (finding that dismissal of the lawsuit was appropriate because the plaintiff failed to claim that a five-month delay was unreasonable).

44 *See In re* Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1146 (N.D. Cal. 2018) ("Without more specific information, the Court cannot evaluate whether Defendants unreasonably delayed in notifying customers about the extent of the 2013 Breach . . . . Plaintiffs' allegations remain insufficient.").

45 *See* Stallone v. Farmers Grp., Inc., No. 2:21-cv-01659-GMN-VCF, 2022 WL 10091489, at *8 (D. Nev. Oct. 15, 2022) ("Defendants' argument [that plaintiffs did not incur injury due to delay] is better suited for a motion for summary judgment when the record is more fully developed."); *see also* Buonasera v. Honest Co., 208 F. Supp. 3d 555, 566 (S.D.N.Y. 2016) ("Courts have generally held that since this second factor requires a reasonableness analysis, it cannot be resolved on a motion to dismiss.").

46 Griffey v. Magellan Health Inc., 562 F. Supp. 3d 34, 56 (D. Ariz. 2021).

unreasonableness at the motion-to-dismiss stage incentivize hasty and sloppy breach notification.[47] A hardline rule that a certain number of days is per se unreasonable pushes businesses to respond as fast as possible, even if they have not properly restored the integrity of the system, determined the scope of the breach, or accurately established data subjects' contact information. If courts wait until they have a record to determine what is reasonable, businesses have a reason to take robust incident response measures, which incentivizes a prudent breach response. The court's review of which measures were reasonably necessary prevents reporting entities from delaying notice in bad faith. Waiting until summary judgment for the right reasons makes breach responses more accurate and more precise.

Notwithstanding the aforementioned 2024 decisions, much of the case law supports this position. For example, the U.S. District Court for the Eastern District of Virginia has opined:

> [W]hether [defendant's] substitute notice was timely is a question not ripe for the motion to dismiss stage. The notice's timeliness is a factual question that asks whether notice of the data breach occurred "without unreasonable delay." Here, the Complaint alleges that it took [defendant] approximately four . . . months to realize that there had been a breach, which, in fact, [defendant] did not itself discover. Moreover, the Complaint alleges that [defendant] could have discovered the hack as early as April, since the hacker . . . had posted her action on an online forum . . . . Further, there is no argument by [defendant] that the law enforcement safe harbor, which permits a delay in notifying affected individuals, applies. In

---

47 An upper limit by which notification must be given "would likely incentivize [companies] to notify individuals quicker than they otherwise would." Michael Bloom, *Protecting Personal Data: A Model Data Security and Breach Notification Statute*, 92 ST. JOHN'S L. REV. 977, 997 (2018).

> But, bright line rules are inflexible. . . . [A]n upper limit may do more harm than good. There may be situations where an entity has the means to notify individuals in much less time than the commonly required thirty days. Including an upper limit on what can be considered "without undue delay" can actually give entities a "cushion to delay notification[]." Some businesses argue that thirty days is too short of a window to assess the extent of and respond to a data breach. In that event, when that claim is true and stands up to scrutiny from federal agencies, a more flexible window would allow entities to delay notification until it would be more proper. As long as it is objectively reasonable that the entities take that much time, it would be fairer to allow them to do so. The uncapped standard provides flexibility to deal with the exigencies of each individualized situation and is the preferable standard for a federal data breach notification law.

Id. (second alteration in original) (footnotes omitted).

> any event, these are all factual questions not suitable for disposition on a motion to dismiss.[48]

Likewise, the Nebraska District Court declined to rule on whether the plaintiff could establish that the delay was unreasonable because it presented a question that went "to the sufficiency of the evidence supporting the allegations in the amended complaint, not the sufficiency of the allegations."[49] Even in California, where some courts have held to the contrary, many have held that the reasonableness of breach notice is "a factual determination not properly decided by the Court on a motion to dismiss."[50]

B. Relying on Precedent to Determine the Number of Days that Is Prima Facie Unreasonable Leads to Impractical Results

If courts follow the "*x* number of days is per se a sufficient allegation of unreasonableness" approach, then results within a state would become incoherent and unjust. For example, if California followed the *Jackson* court's logic, where an allegation of a 139-day delay alone is sufficient to survive a motion to dismiss on its own terms, then the most responsible California company, which conducted a rigorous investigation lasting 140 days in good faith, loses simply because more than 139 days is per se unreasonable. This would be the case even if no one could possibly have completed the investigation sooner.[51] Turn the hypothetical on its head and you get equally ridiculous results. If courts looking exclusively at the timelines hold that 139 days is per se unreasonable, then it is possible to imagine a company that sits on its hands for 138 days while conducting a meager or no investigation, only to send notice at the eleventh hour. Clearly, this result is not desirable, and this delay is not reasonable.

---

48 *In re* Cap. One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 416 (E.D. Va. 2020) (citations omitted).

49 Weisenberger v. Ameritas Mut. Holding Co., 597 F. Supp. 3d 1351, 1365 (D. Neb. 2022) (citing Stamm v. County of Cheyenne, 326 F. Supp. 3d 832, 847 (D. Neb. 2018)).

50 *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 1009 (S.D. Cal. 2014).

51 Of course, this would be an extraordinary situation, and in the vast majority of cases, four-month delays would be difficult to justify. This Article does not claim that a data breach response should take more than a few days or weeks, but rather, it clarifies how courts should determine the appropriate length of a data breach response. *But see* Golubock, *supra* note 6, at 343 ("[C]ourts have permitted reporting of data breaches weeks after the facts of a breach became known.").

The results would be no more comprehensible across state lines. Imagine a hypothetical State *A*, which has case law that only a 45-day or more delay is per se unreasonable. Also imagine a hypothetical State *B*, which has case law that only a 60-day or more delay is per se unreasonable. A 46-day delay would be prima facie unreasonable in State *A* but prima facie reasonable in State *B*. Is there some public policy specific to State *B* that demands an extra 15 days in the grace period? Perhaps, if all the companies in State *B* are so complex and hold data on so many individuals that a longer grace period is desirable. But this seems far-fetched, as does the idea that a 60-day grace period—as opposed to a 45-day grace period—would be top-of-mind for State *B* voters in electing their legislators.

This inconsistency is not just doctrinal—it has real-world harms. First, staying with the State *A*/State *B* hypothetical, companies that participate in interstate commerce would have to follow arbitrarily different timelines for the same investigation, increasing compliance costs and potentially delaying notification for no apparent benefit. This exacerbates the fact that data breaches can lead to astronomically costly litigation. Professors Daniel Solove and Danielle Keats Citron have identified what they call the "multiplier problem," noting that organizations hold data on so many individuals that recognizing even a small amount of harm is multiplied by a staggering number of people such that runaway class actions could bankrupt companies.[52] And for what purpose? The relief provided by slow and expensive class action lawsuits is unlikely to provide meaningful redress to the vast majority of data subjects.[53] Many business advocates, therefore, argue that letting data breach liability off the leash would bankrupt any business, small or large, that holds data. Because unlawful disclosures impact "tens of thousands of individuals[,] . . . [t]he liability faced by an allegedly negligent defendant would be catastrophic in magnitude."[54]

This is not necessarily to say liability for data breaches should be wholly off the table. Rather, this shows that courts

---

52 Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 783 (2018).

53 *Id.*

54 Kenneth S. Abraham & G. Edward White, *Torts Without Names, New Torts, and the Future of Liability for Intangible Harm*, 68 AM. U.L. REV. 2089, 2137 (2019).

must approach data breach liability with extreme caution. Herein lies the proper role of stare decisis in data breach response law: determining which elements of an incident response investigation are reasonable for breaches of which scope and in which sectors. Transparency in what breach response steps are reasonable sets clear guidelines for fostering customer confidence and avoiding liability. Take the example of the hypothetical high-end cyber forensics group, Data Breach Responders Pro, which takes a meticulous—if sometimes slow—approach to cyber incidents. Assume a prior court determined that it was reasonable for Company *X*, a fictional company that suffered a data breach, to retain Data Breach Responders Pro to contain and analyze a breach of one million individuals' protected records. Company *Y*, another fictional company that suffered a data breach of one million individuals' similar records, can confidently retain Data Breach Responders Pro to contain and analyze its own breach without worrying that Data Breach Responders Pro's thorough process will unreasonably delay notice in violation of the law. Likewise, if the case law indicates that certain kinds of data, such as biometric data or Social Security numbers (SSNs), justified a longer period of analysis in Company *X*'s case, then Company *Y* can be equally thorough when dealing with biometric data or SSNs. On the flip side, if an earlier court held that it was unreasonable for Company *X* to take extra time drafting an extensive data breach notification letter given the low risk of harm involved, then Company *Y* knows not to do so.

This approach helps consumers as well. From the individual's perspective, data breach notices are important so that consumers can activate credit monitoring services and take other steps to mitigate the effects of a breach. A substantively inaccurate data breach notification (for instance, what data was compromised, how it was compromised, to whom data was disclosed, and what risks may be present) may mean that individuals retain the wrong kind or degree of identity protection. An underinclusive data breach notification could leave some individuals who should be entitled to protection on the company's dime without any identity protection at all. And an overinclusive data breach notification may cause the company to lose money paying for individuals who have no need to retain identity protection services, while those individuals take time out of their busy lives and endure the emotional stress of suffering identity theft for no reason. Timely, but also thorough and

accurate notice of a data breach, is in both the business' and the consumers' best interest.

C. Ignoring Breach Response Investigations in Favor of a Topline Number of Days Is Inconsistent with the Purpose of Data Breach Response Statutes

Data breach notification statutes do not permit delay for delay's sake but rather so that companies have time to determine root causes and take responsible steps toward remediation. Therefore, a peek under the hood is most consistent with the statutory purpose of data breach laws. Some data breach notification statutes explicitly tie reasonableness to the investigation. For example, Alabama's statute states that "[n]otice to individuals . . . shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation."[55] In states like Alabama, the importance of the investigation is obvious. Yet, as previously discussed, other states favor an approach that simply requires notification to be provided "without unreasonable delay."[56] This approach, too, serves as an implicit authorization for investigation if none exists in the statute and, by extension, a built-in explanation of what delay is unreasonable.[57] Researcher Carol Hayes has argued that the phrase "without unreasonable delay" is preferable to phrases like "as quickly as possible" or "as soon as possible" because it "allows for reasonableness considerations to be a factor in enforcement."[58] She explains:

> The focus on unreasonable delays implies that there could be a reasonable delay. Forty-two of the analyzed laws include language suggesting that a reasonable delay would include time to recover from the breach. This is commonly phrased to include time to determine the scope of the breach and time to restore system integrity. All of the analyzed data breach laws included explicit language allowing for delays due to a law enforcement investigation related to the breach.[59]

---

55 ALA. CODE § 8-38-5(b) (2025).

56 *See supra* Part II.

57 Dana J. Lesemann, *It's Not the Breach, It's the Cover-Up: Using Digital Forensics to Mitigate Losses and Comply with Florida's Data Breach Notification Statute*, 82 FLA. BAR J. 20, 24 (2008).

58 Hayes, *supra* note 12.

59 *Id.* (footnote omitted).

Investigations are so core to breach response that in some states, failure to conduct a good faith investigation is itself a violation. Kansas' notification statute reads:

> A person that conducts business in this state . . . that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused.[60]

Regardless of how it is styled, all of these approaches center the "who, what, when, where, and how" of the breach response and investigation. Time and breach response go hand in hand. For courts to get the issue right, and to effectuate the purpose of the statutes, they must consider the defendant's investigation.

IV. COURTS MUST INTERROGATE THE ELEMENTS OF A DEFENDANT'S DATA INCIDENT RESPONSE TO DETERMINE WHETHER DELAY IS UNREASONABLE

If courts cannot rely on precedent to determine how many days is per se reasonable, how should they answer the question? Courts must do the sometimes painstaking work of considering the facts of the defendant's response to the breach. Among other factors, this may involve determining: the nature of the information compromised (for instance, comparing protected health information to a date of birth, zip code, or SSN); who gained unauthorized access to the data; the risk of harm presented by disclosure; the number of individuals affected; the availability and accuracy of those individuals' contact information; whether or not the defendant retained counsel; the identity, capabilities, experience, and financial cost of counsel; which systems were affected; how those systems were affected; the complexity of those systems; the time required to restore the integrity of such systems; the level of detail required in the notice to satisfy the reporting requirement; and more. Many state statutes explicitly list what factors are to be analyzed when determining the reasonableness of the response. For example, Hawaii's data breach notification statute requires notification to be made "without unreasonable delay, consistent with . . . any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable

60 KAN. STAT. ANN. § 50-7a02 (2025).

integrity, security, and confidentiality of the data system."[61] Courts in states like Hawaii have an easy place to start. Courts in states whose statutes do not enumerate factors can borrow from this guidance in conducting more informed inquiries.

Much of the scholarship has endorsed this approach. Hayes has endorsed a flexible "without unreasonable delay" standard, with the important modification that states clarify which causes for delay are reasonable.[62] She suggests a three-part reasonableness standard for data breach notification delays:

> First, a delay is reasonable if it is necessary for law enforcement purposes. . . .
>
> The second and third parts of the reasonableness standard focus on the data collector's investigation and system restoration. A delay should be considered reasonable if it is necessary to determine the scope of a data breach. This is important because the scope determination is central to data breach notification obligations. A delay should also be considered reasonable if it is necessary to restore the integrity of the affected system. It is important to include recovery time within a reasonableness standard because unless system integrity is restored, a data breach cannot truly be said to be "over."[63]

Likewise, Professors Scott L. Shackelford, Anne Boustead, and Christos Makridis have advocated for "an empirically grounded, flexible approach" to cybersecurity that prioritizes combining cybersecurity best practices and efforts to inform consumers of their rights and the importance of exercising them.[64] Finally, this approach is no harm, no foul for the affected individuals. A court's reasonableness review of the facts will make it unlikely that companies will delay sending notices any more than under the current regime. As previously discussed, for individual litigants, the immediate practical result is the same: denial of a motion to dismiss and resolution of the issue at summary judgment or later.

V. CONCLUSION

Without a general federal data incident reporting statute, making progress in breach notification law is arduous. The decentralized nature of data breach law requires courts and regulators in over fifty jurisdictions to agree on a complex and

---

61 HAW. REV. STAT. § 487N-2 (2025).
62 Hayes, *supra* note 12, at 1276.
63 *Id.* at 1276–77.
64 Shackelford, Boustead & Makridis, *supra* note 13, at 90.

nuanced approach. That the approach explained in this Article asks courts to volunteer for sometimes grueling case-by-case factual analysis only makes it a harder pitch. However, a better approach to what constitutes an "unreasonable" delay in data breach notification statutes—one that focuses on a reporting entity's breach response instead of a topline number of days—is needed to fulfill the purpose of the laws, help businesses maintain compliance, and protect consumers from identity theft.