

Loyola University Chicago, School of Law

LAW eCommons

Faculty Publications & Other Works

2025

Unto the (Data) Breach

Charlotte A. Tschider

Loyola University Chicago School of Law, ctschider@luc.edu

Follow this and additional works at: <https://lawecommons.luc.edu/facpubs>



Part of the [Computer Law Commons](#), [Litigation Commons](#), and the [Torts Commons](#)

Recommended Citation

Charlotte A. Tschider, Unto the (Data) Breach, 59 U. Rich. L. Rev. 591 (2025).

This Article is brought to you for free and open access by LAW eCommons. It has been accepted for inclusion in Faculty Publications & Other Works by an authorized administrator of LAW eCommons. For more information, please contact law-library@luc.edu.

UNTO THE (DATA) BREACH

Charlotte A. Tschider *

ABSTRACT

Since the early 2000s, U.S. courts have begun hearing “data breach” liability cases, the inevitable result of a growing internet-connected technology infrastructure. The relatively recent development of case law signals a body of law in development, stunted by significant limiting factors that prevent the coalescence of legal principles. To date, no holistic empirical exploration of data breach cases has offered sufficient detail to explore these factors. This descriptive empirical study analyzes, in detail, 225 data breach cases from 2005–2022, reviewing these cases over an extended period to descriptively identify key trends and changes within a bona fide data breach case’s life on the docket.

This study tests common perceptions of data breach litigation, including Article III standing challenges that have presented a nearly insurmountable obstacle to data breach litigation. This study also identifies the type of plaintiff, settlement amounts, type and disposition of information compromised, claims, common motions, and key strategies most likely to result in a favorable plaintiff outcome, including key impediments. These results will provide crucial information for litigating parties, their counsel, judges, and policymakers.

* Charlotte Tschider is an Associate Professor of Law at the Loyola University Chicago School of Law. I would like to thank David Schwartz, Josephine Wolff, Mark Lemley, Christopher Yoo, Mark McKenna, Bryan Choi, Brett Frischmann, Matthew Sag, Justin (Gus) Hurwitz, David Thaw, Steven Bellovin, and participants in the 2024 Junior Faculty Forum for Law and STEM for comments on various stages of this Article. A special thanks to Jay Edelson and Aaron Charfoos for their perspectives on data breach litigation and for offering their expertise with my classes on this topic. I would especially like to thank Annalisa Kolb for her exceptional research skills generating and validating cases in this study. For access to the full data set, please contact me at ctschider@luc.edu with the subject “Data Breach Study.”

TABLE OF CONTENTS

INTRODUCTION	594
I. STUDY METHODOLOGY.....	599
A. <i>Literature Review</i>	599
B. <i>Methodology</i>	603
C. <i>Limitations</i>	607
D. <i>Corpus Overview</i>	608
II. FINDINGS	609
A. <i>Cases and Circuit</i>	610
1. Case Timing and Disposition.....	611
2. Plaintiff Types and Data Types.....	612
3. Procedural Position	615
B. <i>Standing</i>	615
1. Background	616
2. Standing and Harm Status: 12(b)(1).....	621
3. Theories of Harm and Damages.....	624
4. Failure to State a Claim: 12(b)(6)	626
C. <i>Claims</i>	627
1. Claim Variation and Average Claims per Case.....	628
2. Successful Claims	629
3. Tort Law and the Economic Loss Doctrine	630
4. Contract Law	639
5. State and Federal Claims	644
6. Combined Claims.....	647
7. Class Certification	648
8. Claims Overall	649
D. <i>Settlement</i>	650
III. FUTURE INQUIRY.....	654

2025]	UNTO THE (DATA) BREACH	593
A.	<i>Confirmations and Observations</i>	654
B.	<i>New Contributions</i>	655
1.	12(b)(6) Standing: A New Frontier.....	656
2.	Claim Types and Court Preferences	657
3.	The Influence of the Federal Trade Commission	662
4.	Settlement.....	663
5.	Identity and Credit Monitoring.....	665
CONCLUSION.....		665
APPENDIX: CASE LIST		667

INTRODUCTION

In 2017, cyber attackers exfiltrated hundreds of millions of customer records from Equifax, a for-profit credit-monitoring agency responsible for storing the highly sensitive financial and personal records of credit-seeking Americans.¹ As one of three credit-monitoring agencies providing credit scores—the basis of which determine creditworthiness for financial institution creditors, mortgage companies, landlords, and employers—Equifax stored extremely sensitive personal and financial data.²

Almost immediately following the breach's announcement, aggrieved customers brought lawsuits against Equifax, totaling at least sixty class action lawsuits.³ Ultimately, the Equifax breach resulted in one of the largest settlements in history: \$600 million from a multi-jurisdictional case involving a coalition of state attorneys general that created a victim compensation fund.⁴

The Equifax data breach became a bellwether for data breach litigation, illustrating just how big and impactful a data breach could be while also signifying the complexity of resulting litigation. Not only did customers sue Equifax in class-action lawsuits, Equifax also faced lawsuits from individuals who had not registered with Equifax (though Equifax had maintained their records for credit monitoring), business customers, shareholders, state attorneys general, the Federal Trade Commission ("FTC"), Consumer Financial Protection Bureau, and the Securities and Exchange Commission.⁵ The Equifax cases illustrated that data breach litigation can be multifaceted and complex.

1. Josh Fruhlinger, *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO ONLINE (Feb. 12, 2020), <https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html> [<https://perma.cc/PQA5-76QW>].

2. Caitlin Kenny, *The Equifax Data Breach and the Resulting Legal Recourse*, 13 BROOK. J. CORP. FIN. & COM. L. 215, 221 (2018).

3. *Id.* at 224.

4. Press Release, Pa. Att'y. Gen., AG Shapiro Secures \$600 Million from Equifax in Largest Data Breach Settlement in History (July 22, 2019), <https://www.attorneygeneral.gov/taking-action/ag-shapiro-secures-600-million-from-equifax-in-largest-data-breach-settlement-in-history/> [<https://perma.cc/W95Z-QVSC>] (noting that the \$600 million settlement includes a Consumer Restoration Fund of up to \$425 million and a \$175 million payment to the states).

5. See Kenny, *supra* note 2, at 222–24; Press Release, Fed. Trade Comm'n., Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data

Despite the complexity of modern data breaches, they are not a recent occurrence. For as long as modern computer systems have existed, so have individuals who compromise them.⁶ The 1990s introduced the broad expansion of digitized information,⁷ opening the door to attackers seeking to fulfill some motive; for example: to profit financially, damage organizations and their reputation, compromise U.S. interests, or simply to compete with and beat other attackers.⁸

Modern data breaches occurred as attackers compromised exposed and virtually connected databases in the late 1990s and early 2000s.⁹ In response to this emerging problem, California used the term “database breach” in the first U.S. data breach notification statute (2002), obliging organizations to notify affected individuals when their data is compromised.¹⁰

Breach (July 22, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach#:~:text=Equifax%20Inc.%20has%20agreed%20to%20pay%20at%20least,in%202017%20that%20affected%20approximately%20147%20million%20people> [https://perma.cc/252M-FPXC]; Press Release, U.S. Sec. & Exch. Comm’n., Former Equifax Executive Charged with Insider Trading (Mar. 14, 2018), <https://www.sec.gov/news/press-release/2018-40#:~:text=The%20Securities%20and%20Exchange%20Commission%20today%20charged%20a,personal%20information%20of%20about%20148%20million%20U.S.%20customers> [https://perma.cc/K8JN-955L].

6. Hacks of the French Telegraph system occurred as early as 1834, while the first cyberattacks quickly followed the first Internet connections at least as early as 1971. *Cybersecurity History: Hacking & Data Breaches*, MONROE UNIV., <https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches> [https://perma.cc/G742-7B3X]. Although data breaches technically existed in the 1980s and 1990s, they were relatively small and resulted primarily from accidental exposure and misuse of existing access. *Id.* These early-era data breaches involve, for example, employees of a hospital looking at family members’ data without authorization. *Id.*

7. M.F. Bregman, *A Ten Year Outlook on Technology*, PROC. ELEC. TECH. DIRECTIONS TO THE YEAR 2000 2, 2 (1995).

8. Chisolm Ikezuuora, *Inside the Hacker’s Mind: Analyzing the Psychology Behind Cyber Attacks Leading to Data Breaches*, PRIVACYEND, <https://www.privacyend.com/psychology-behind-cyber-attacks-leading-data-breaches/> [https://perma.cc/4P9G-ARKR].

9. See Katie Chadd, *The History of Cybercrime and Cybersecurity, 1940–2020*, CYBERCRIME MAG. (Nov. 30, 2020), <https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/> [https://perma.cc/H38E-HA5F]. The cause of such data breaches has fallen into a myriad of categories, including malicious insiders, malicious outsiders, hacktivists, nation-state, and accidental losses/human error (that nevertheless resulted in adverse parties accessing data). See Lauren M. Lozada, *The (Possibly) Injured Consumer: Standing in Data Breach Litigation*, 93 ST. JOHN’S L. REV. 461, 464 (2019).

10. Timothy H. Skinner, *California’s Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, RICH. J. L. & TECH., Fall 2003, ¶1, ¶3. See generally 45 C.F.R. § 164 (2023) (requiring the Department of Health and Human Services to notify individuals when their personal data was subject to a cyber breach); 12 C.F.R. pt. 225, app. F. (2024) (requiring banks to implement technological safeguards).

In the early 2000s, administrative agencies regulating entities with sensitive personal information adopted data breach notification rules containing similar language.¹¹ As data breaches continued to increase in frequency, legal academics began examining the growing legal challenges in these cases.

While all U.S. states have adopted data breach notification statutes, and an increasing number of privacy statutes have recently emerged,¹² contemporary data breach liability is largely a creature of the common law. To date, no omnibus, broadly applicable federal statute establishes explicit requirements for organizations and clarifies their duties with respect to business customers, consumers, or shareholders.¹³ Under state law, there is no omnibus state statute specifying technical requirements for these organizations either.¹⁴ Because very few statutes apply broadly and data breaches challenge legal doctrine, courts are, even if slowly and reticently, developing a new and distinct area of the law.

11. Skinner, *supra* note 10, ¶ 62; 45 C.F.R. § 164.404(a)(1) (2024); 12 C.F.R. pt. 225, app. F.

12. See, e.g., CAL. CIV. CODE § 1798.150 (2024); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1302; Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575 (Cum. Supp. 2024). Nineteen states have adopted privacy laws in recent years. See *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PROS., <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#~:text=State-level%20momentum%20for%20comprehensive%20privacy%20bills%20is%20at%20an%20all-time> [https://perma.cc/U6TK-3XLT].

13. Although the Federal Information Security Management Act (FISMA) creates specific cybersecurity requirements for federal systems through the National Institute of Standards and Technology (NIST), it does not apply generally to private organizations or publicly traded corporations. See *generally* Federal Information Security Management Act, 44 U.S.C. § 3551. Some of these organizations may, by virtue of doing business on behalf of the federal government and by obligation through contract, implement these requirements. But there is no direct evidence demonstrating that even these organizations with government contracts extrapolate these same security requirements across the organization for other lines of business. It is well-known that the United States, at least in federal law, generally addresses both privacy and security through sectoral (or sector-specific) rather than broadly applicable statutes.

14. Scott Shackelford, Annie Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, COUNCIL ON FOREIGN RELS. (Mar. 7, 2022), <https://www.cfr.org/blog/defining-reasonable-cybersecurity-lessons-states> [https://perma.cc/K76W-6UGV]; see CAL. CIV. CODE § 1798.150. California appears to be the first state that is interpreting general "reasonable security" language promulgated by the California Privacy Protection Agency ("CPPA") and passed under the California Consumer Privacy Act ("CCPA") and its successor, the California Privacy Rights Act ("CPRA"). The CPPA held pre-rulemaking activities on cybersecurity audits, risk assessments, and automated decision-making in February of 2023 and is expected to eventually issue associated rules to interpret this language.

However, there are many challenges in data breach litigation; these challenges are the largely confounding focus of many well-respected academics in the cybersecurity, privacy, and data protection law fields.¹⁵ This attention has much to do with data breach litigation's unusual blend of legal doctrine, overlapping with many specializations: tort law, contract law, corporate law, securities regulation, and administrative law. Unlike the "law of the horse,"¹⁶ data breach litigation applies existing legal doctrine to new factual and contextual circumstances, illuminating new meaning and pushing the limits and understanding of that doctrine.¹⁷

Principally, data breach litigation blends two distinct areas of legal expertise: privacy law and cybersecurity law.¹⁸ Although cybersecurity incidents can involve compromise of any type of proprietary or valuable internal information, data breach litigation concerns the personally identifiable data of natural people.¹⁹ Distinct from traditional privacy law concerns—such as questionable notice of disclosure, impermissible data collection, and unauthorized use—data breach issues usually involve the criminal actions of a third party intervening in otherwise permissible data practices.²⁰ The events that give rise to data breach litigation are quite unusual: both plaintiffs and defendants have experienced harm due to criminal behavior.²¹ Data breach litigation is distinct from other

15. See generally Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295 (2019) (examining duty and injuries for negligence actions); George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1 (2016) (examining the nature of data breach harm); Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C. J. L. & TECH. 1, 44–64 (2021) (establishing a framework for examining psychological harm in data breach litigation).

16. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 501 (1999).

17. *Id.* at 502.

18. See generally Charlotte A. Tschider, *Locking Down "Reasonable" Cybersecurity Duty*, YALE L. & POL'Y REV., 2023, at 75 (differentiating between data breaches implicating personal information and cyberattacks and incidents affecting data other than personal information).

19. As Derek Bambauer explains, privacy is typically a normative determination, which is consistent with how we treat people: who should have access and the ability to alter information; however, security is a "set of technological mechanisms." Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 669 (2013). Data breaches couple these considerations together.

20. "Third parties" may be internal or external attackers.

21. U.S. FED. BUREAU OF INVEST., INTERNET CRIME REPORT 3 (2021), https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf [<https://perma.cc/HYT6-M56A>].

cases involving unauthorized disclosure, such as an employee sending a file to an incorrect customer.

However, defendant organizations may be responsible for foreseeable criminal behavior that affects consumers, employees, patients, and other organizations in a business relationship with them.²² Most data breach litigation is premised on the idea that these organizations should have used appropriate precautions and a reasonable duty of care to prevent cyberattacks.²³ Additionally, defendants may be responsible for actions that resulted from a failure to take some action they were obligated to perform by statute or by contract.²⁴

Because data breach litigation involves various doctrinal areas of the law, academics have examined many themes involving plaintiff status and the types of claims they raise. Although Article III standing has occupied the most attention, a variety of other subjects have also emerged, including remarks on preferable claim types (and impediments), cybersecurity duties, and damages theories.

This paper examines a nearly twenty-year arc in data breach litigation, analyzing 225 verified data breach cases to observe these trends. Part I describes previous empirical research on this topic, study methods, and limitations. Part II introduces broad trends and specific findings to challenge perspectives of examined legal conventions and doctrine. Part III concludes by crystallizing

22. See, e.g., *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1309–10 (D. Minn. 2014) (describing Target Corporation's obligations based on foreseeability of harm and referencing external credit-card industry security requirements); *Hapka v. Carecentrix, Inc.*, No. 16-2372-CM, 2016 U.S. Dist. LEXIS 175346, at *13 (D. Kan. Dec. 19, 2016) (explaining that reasonable foreseeability of harm triggers a duty of care on the part of the defendant).

23. See, e.g., *Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-186-CHB, 2020 U.S. Dist. LEXIS 8514, at *6, *8 (W.D. Ky. Jan. 17, 2020) (describing the occurrence of unauthorized access to plaintiff data as the basis for the defendant not performing their duty); *Buckley v. Santander Consumer U.S.A., Inc.*, No. C17-5813 BHS, 2018 U.S. Dist. LEXIS 53411, at *13–14 (W.D. Wash. Mar. 29, 2018) (describing the common-law duty of businesses to protect customers from imminent and foreseeable criminal conduct); *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1366 (S.D. Fla. 2015) (finding that the defendants undertook a duty with respect to the plaintiffs and were obligated to perform that duty).

24. See, e.g., *Pa. State Emps. Credit Union v. Fifth Third Bank*, No. 1:CV-04-1554, 2006 U.S. Dist. LEXIS 40066, at *1 (M.D. Pa. June 16, 2006) (finding a duty where contract specifies security obligations, here in relation to bank contracts and external credit card industry security requirements); *Cnty. Bank of Trenton v. Schnuck Mkts., Inc.*, 210 F. Supp. 3d 1022, 1038–39 (S.D. Ill. 2016) (identifying a duty as extending from an implied contract).

the findings of this study to offer preliminary conclusions and offer avenues for future research.

I. STUDY METHODOLOGY

Despite the substantial focus on data breach liability cases, to date, scholars have only explored data breach liability over a limited time period and for a subset of litigation information. To provide ample information to test the validity of academic observations in connection with prevailing litigation themes described in Part II, this study examined cybersecurity data breach cases from the first case explicitly referring to “data breach” in 2005 until 2022.

This study aims to (1) identify factors that could influence a plaintiff’s likelihood of success against a defendant that has experienced a data breach, and (2) provide observations of the overall evolution of the data breach litigation ecosystem. The key objective of this study is to provide potential parties, litigating attorneys, courts, and policymakers with relevant information about the current state of data breach litigation. It also informs academics who promote specific changes in data breach litigation using accurate information.²⁵

A. *Literature Review*

Despite the relative ubiquity of data breaches and associated lawsuits, very few empirical studies have been conducted on this precise topic. Although research has been completed about various issues related to data breaches, only two empirical studies with slightly different methodologies have examined data breach lawsuits. These studies offer useful points of contrast for evaluating the results of this study.

Sasha Romanosky, David Hoffman, and Alessandro Acquisti conducted the first empirical study on data breach litigation in 2014, analyzing a data set of more than 230 cases, concluding in

25. Although this study does provide useful descriptive information, the data set’s size is not large enough to offer predictive analytics. Therefore, it is premised as a “descriptive empirical” study.

2010.²⁶ Romanosky et al. sought to provide rich, descriptive information while also answering two key research questions: (1) what kinds of data breaches are being litigated in federal court and why, and (2) what kinds of cases are settling and why.²⁷

Central to the Romanosky et al. study is the nature of the compromise giving rise to litigation. Within a broad definition, “data breach” cases could include various fact patterns, including human errors like losing a laptop or improperly disposing of personal information.²⁸ One hypothesis of the Romanosky et al. study theorizes that improper disclosure or disposal of personal information increases the strength of negligence claims.²⁹ Overall, this approach includes a variety of cases with less complex fact patterns than only data breach cases involving a cyberattack.³⁰

The Romanosky et al. study found that specific characteristics apply to cases involving “unauthorized disclosure.”³¹ First, plaintiffs seek relief for past financial harm tied to fraud, emotional distress, or the potential for future harm, but these harms largely are not effectively claimed, resulting in settlement.³² Additionally, most lawsuits are private and most defendants are large for-profit entities (usually businesses).³³ Finally, plaintiffs bring a wide variety of claims including both common law and statutory bases for these claims.³⁴

This study also identified other metrics, such as increased odds of a firm being sued related to financial losses, and a lower risk of being sued when free credit monitoring is offered.³⁵ Consistent with the breadth of this study, Romanosky et al. also found a

26. Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 76 (2014).

27. *Id.*

28. *Id.* at 84.

29. *Id.*

30. *Id.* The fact patterns include improper disclosure or disposal of personal information, a computer hack, or loss or theft of hardware. *Id.* The search terms Romanosky et al. used in Westlaw included “personally identifiable information” or “personal information,” and “data breach,” “security breach,” or “privacy breach.” *Id.* The researchers then manually reviewed the cases to ensure they included legitimate unauthorized disclosure of personal information. *Id.* at 79.

31. *Id.* at 76.

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

greater likelihood of cases being brought when data is improperly disposed or when financial data are compromised than when breaches are due to lost or stolen data of other types.³⁶ Additionally, the study identified key settlement details connected to the status of class action lawsuits (certified classes increased settlement), how the data was compromised (more cyberattacks were settled), and the type of data compromised (medical data increased settlement probability).³⁷ Despite this study adopting broader search criteria than the present study, much of the Romanosky et al. study was roughly confirmed.³⁸

The most recent empirical data breach litigation study, conducted by Dominik Molitor, Wullianallur Raghupathi, Aditya Saharia, and Viju Raghupathi, used machine learning to mine data breach cases, adopting a similarly expansive approach. Molitor et al. included an extremely broad collection of data breach cases, including cases of internal noncompliance, over a ten-year period ending in 2021.³⁹ Molitor et al. also used a combination of search terms, such as “cybersecurity,” “data breach,” and other terms via a Westlaw search to total 698 cases.⁴⁰ The team then used machine-learning techniques to mine the documents.⁴¹

The study revealed key terms that were used across documents, including “identity theft,” “breach,” and “injury,” which were the most frequent.⁴² Using a more fine-tuned methodology that identifies co-occurring terms, “data breach,” “breach contract,” “data security,” and “credit card” were dominant words in the corpus.⁴³ Phrases used most frequently included “customer data security,” “social security number,” “risk identity theft,” “federal rules civil,” and “economic loss doctrine.”⁴⁴ Overall, the study created a more comprehensive corpus using Westlaw than the Romanosky et al. study largely because it included a greater variety of cases that

36. *Id.*

37. *Id.* at 76–77.

38. *See infra* Part II.

39. Dominik Molitor, Wullianallur Raghupathi, Aditya Saharia & Viju Raghupathi, *Exploring Key Issues in Cybersecurity Data Breaches: Analyzing Data Breach Litigation with ML-Based Text Analytics*, INFO., Nov. 2023, at 1, 2–3, MDPI, Art. No. 600.

40. *Id.* at 7.

41. *Id.* at 8–9.

42. *Id.* at 11.

43. *Id.* at 17.

44. *Id.* at 18.

may not have been bona fide data breach cases or related to data breaches *per se*. For example, Molitor et al. report the terms stakeholders (litigants) most care about are: “identity theft,” “hacker,” “negligence,” “FCRA,” “cybersecurity,” “insurance,” “phone device,” “TCPA,” “credit card,” “merchant,” and “privacy.”

Because the nature of the machine-learning approach did not involve manual validation, these terms could indicate cases not specifically related to a data breach. For example, the FCRA and TCPA involve privacy interests but do not involve data breaches; rather, they involve organizations not fulfilling obligations concerning personal information (FCRA related to consumer credit reporting data, TCPA related to telephone-based auto-dialing).⁴⁵ “Insurance” could relate to litigation involving organizations attempting to secure insurance payouts for data breaches.⁴⁶

The present study responds to both the time that has elapsed since Romanosky et al.’s study, which concluded prior to the “golden age” of data breach litigation following the Target Corporation data breach.⁴⁷ It also aims to focus on bona fide data breaches involving confirmed data exposure, exposed as a result of the intentional actions of an attacker. Although a more expansive definition of data breach may have been appropriate for research questions comparing the nature of the breach and plaintiff success—as Romanosky et al. did—to more closely focus on the nature of harm, standing, and claim success for cases involving intervening and typically criminal actions, a more precise definition is appropriate. This unique nuance creates unusual circumstances for many data breach cases that can affect questions of duty, obligation, and causation. Specifically, this study aimed to examine these concepts in a more detailed way by examining the nature of distinct plaintiff claims and court responses to these claims, extending both Romanosky et al. and Molitor, et al.’s findings. However, upon discovering that very few cases discussed duty, obligation, and

45. Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681, 1681a–1681t; Telephone Consumer Protection Act of 1991 (TCPA), 47 U.S.C. §§ 152, 227, 331.

46. Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), <https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem> [<https://perma.cc/JY59-J52T>]; Alexei Alexis, *Cyber Insurance Gaps Stick Firms with Millions in Uncovered Losses*, CFO DIVE (Apr. 17, 2024), <https://www.cfodive.com/news/cyber-insurance-gaps-stick-firms-millions-uncovered-losses-cybersecurity-cyberattack/713531/> [<https://perma.cc/EKM5-Z7JC>].

47. See Molitor et al. *supra* note 39, at 2.

causation in much detail, this study was expanded as a descriptive study offering a detailed analysis of harm, standing, and broad claims.

B. *Methodology*

This descriptive empirical study was designed to illuminate potential factors that increase the probability of plaintiff success in data breach litigation, specifically focusing on examining harm, standing, claim prevalence, and claim success. As a secondary complementary examination where data could be gathered, this study also identified when cases conclude, when cases settle, and the settlement amount.

Given its history of providing useful information for purposes of litigation research and its previous use in both empirical studies described in Section A, this corpus was assembled using Westlaw as the initial source of truth to identify a first data set. This corpus was reevaluated five times between May 2017 and December 2023: four instances between May 2017 and July 2020 were used to compile the original data set,⁴⁸ and one final search compiled the extended data set on December 31, 2021. These cases were confirmed in 2023. The analysis process followed these steps:

(1) Data Breaches: An initial compilation of data breach numbers was collected from Statista.

(2) Complete Case Data Compilation: The initial data set was compiled annually over three years (2018, 2019, 2020), including new cases that had completed a three-year “lifecycle” in court, with a confirmatory review of all cases concluding in 2023. Despite the fast pace of initial motions, a three-year lifecycle was used to ensure that most cases had concluded by the time the data was aggregated.

(3) Data Confirmation: Second and third coders (confirmatory review from the person who identified the initial case) reviewed each case in the data set to ensure consistency and verify accuracy.

48. It should be noted that current searches of Westlaw may have changed the data-set volume, as cases are added on an ongoing basis from state and federal courts. During the data collection process, additional cases were added from earlier searches: for example, although a 2017 search would have identified a 2015 case, a 2015 case did not appear in Westlaw until 2019.

(4) Corpus Completion: The preliminary complete data set was complemented with PACER records for specific cases to fill in Westlaw gaps, such as claims pleaded and whether settlement had occurred.

(5) Corpus Validation: The data set was revisited two additional times to identify cases that developed after their three-year lifecycles.

(6) Data Details: A Google search was used to identify settlement details and characteristics of data breaches not included in court filings such as number of records impacted or details of the compromise.

(7) Corpus Extension: An additional year of data breach litigation cases was added to the data set to examine shifting discussion of standing and harm, as well as claims brought, after Supreme Court of the United States decisions during this time.

(8) Data Analysis: Data were analyzed across districts, circuits, state courts, and federal courts for purposes of understanding broad trends from the perspective of plaintiffs. However, some of this data set may have been incomplete in its reporting to Westlaw, resulting in more data compilation representing federal courts.⁴⁹

The first corpus was populated by searching solely for the term “data breach” and including all cases until they could be analyzed in detail. This decision, informed by previous studies with more expansive search terms, aimed to reduce the number of cases involving employee mistakes or exposures that did not involve an attacker’s intentional acts. These cases, compiled over four separate searches, were Shepardized to identify predecessor, precedential, and citing cases,⁵⁰ cases combined into multi-district litigation, and cases combined into class-action lawsuits, regardless of publication

49. See *infra* Section I.C. Similar to the Romanosky et al. study, state court decisions were included. Romanosky et al., *supra* note 26, at 79, 99. However, for analysis of data affecting districts and circuits and questions of Article III standing, state court decisions would not have provided useful details. As illustrated in Part II, state court cases were relatively low in numbers. See *infra* Part II.

50. Shepardizing is a process for identifying cases that cite the case you are reviewing, the cases it cites, and identifying other cases that confirm or deviate from the case’s holding or legal reasoning. Classically, Shepardizing is used to determine precedential effect of a case and distinguishing factors between cases. See *Shepardize*, CORNELL L. SCH. LEGAL INFO. INST., <https://www.law.cornell.edu/wex/shepardize> [<https://perma.cc/HGE7-A3R6>]. This provides a means for identifying other cases that may share the same subject matter but for some reason are not identified by the Westlaw search engine.

status.⁵¹ Each case was then analyzed to ensure it referenced a data breach involving external exposure of personal information. Coders included the Author and research assistants who had completed a cybersecurity law course and received basic training on navigating Westlaw for research purposes. Case details were recorded by the individual searching using the “data breach” query, verified by another member of the research team, then re-verified by the Author to ensure consistency in case details.

Although Westlaw provides a fulsome basis for research, this process resulted in substantial information gaps. For example, available cases often did not include pleadings, or a case might simply document a court decision referencing an earlier motion published separately. Where incomplete information appeared in Westlaw, the case was cross-referenced with PACER records. PACER provides additional detail to explore cases identified from Westlaw, such as complaints, procedural position, motion determination, settlements, amendments, removal, or class certification throughout a case’s life on one or more dockets. Although information about class certification may have been collected, it was not the focus of this particular study; details about it may be partial in nature. PACER was reviewed at the conclusion of a three-year lifecycle; for example, PACER was used in 2020 to review cases brought in 2017.

Because this study was designed to evaluate litigation developments for data breach cases involving harm, standing, and claims, the initial pass of all cases validated that the cause of action was directly related to the “bona fide” data breach involving attacker compromise, rather than data leakage or other privacy issues. Cases that resulted in compelled arbitration before any other pre-trial motions occurred, as well as other cases that involved the terminology “data breach” but were not based on data breach claims, were removed from the data set and maintained in a “cases eliminated from data set” spreadsheet.

51. Although Westlaw is an excellent resource, there are some limitations regarding its complete and accurate assembly of all data breach cases. For this reason, I individually searched for cases where information was incomplete. The initial corpus was identified through Westlaw. This means that, for a full empirical study, some cases may not be included. However, for purposes of evaluating overarching trends in terms of duty and other case outcomes in a more descriptive matter, the corpus fits the overall purpose.

Data collected for each case included general information, such as the court hearing the case, whether the case was appealed, the point in trial at which the case concluded, the date of first and final cases, number of records affected, type of plaintiff affected, data classification, and the claimed unreasonable practices giving rise to the data breach. The data set included harm theories and differentiating factors such as the presence of a privacy notice or security policy, lost benefit of the bargain, lost value of personally identifiable information (“PII”), whether injury claimed was characterized as past or future, or standing raised as 12(b)(1) and 12(b)(6) motions to dismiss. Data also contained claims that included state laws and state common law, despite most cases originating or being transferred to federal court. Finally, this study aimed to collect information that might inform organizational practices, such as commentary on duty and reasonable or unreasonable security practices.

Members of the research team analyzed cases in three separate iterations for each of the four data-gathering events (a minimum of three reviews for each case, with re-verification of the entire corpus at each data-gathering event). This iterative, confirmatory analysis identified new developments in previously recorded cases and new cases filed.⁵² Where multiple cases were consolidated by courts, the cases were consolidated in the final corpus as well. This consolidation reduced final case counts because some data breaches precipitated numerous cases later consolidated by federal courts.

A final review of the entire corpus was conducted at the completion of the data set in 2023 for purposes of publication. In total, 172 consolidated, complete “data breach” cases had finished a three-year lifecycle in 2022, with the final cases completing this lifecycle initially filed in 2019.

Due to important cases that could inform data breach litigation, specifically those involving standing determinations by the Supreme Court of the United States, additional cases filed in late 2020 through 2021 created an “extended” data set. This data set

52. This approach could result in greater accuracy in earlier cases than later ones, in part because earlier cases received a greater number of confirmatory reviews. However, this may also have improved accuracy overall because cases reviewed later benefitted from reviews of earlier cases that improved skills of the research team.

extended cases as filed (e.g., claim types), but cases were not included in analyses dependent on case completion, such as standing determinations or case outcomes that could have been overturned later. The combined data set totaled 225 cases, including both the complete three-year data set and the extended data set. Therefore, case details referenced in Part II may be notated for the year of filing or may be notated later upon case conclusion. For example, claim types would be analyzed from the combined data set (including both initial and extended data sets) because the extended data set could faithfully provide accurate information early in the case lifecycle.⁵³ However, to measure case outcomes, analysis was restricted to only cases that had completed the three-year lifecycle to minimize decisions that were “too early,” including for settlement, amended complaints, or the possibility of appeal.

Additional information, such as case-settlement information and data breach details (e.g., size and data compromised) were derived from a combination of public search (Google search) cross-referenced with official court records. This Google search was needed to fill out details related to the type of data compromised, how the data was compromised, and settlement. The research team placed higher value on reputable news agencies and known cybersecurity expert reports where conflict occurred, though no known substantial conflicting information was identified. Information about data breach frequency was derived from Statista.⁵⁴ Some settlement actions have not been disclosed or may still be in active discussions by the conclusion of this study.

C. Limitations

This study included various choices to select a data set that could inform observations regarding harm, standing, and claims for data breaches involving cybersecurity attacks. One important limiting factor involved the search criterion of “data breach” as the sole query in Westlaw. Although scholars previously included more search terms; this study included only the search criterion of “data

53. As the goal of this study is to broadly understand data trends, this avoids misattribution by reflecting later decisions (for example, after a standing case) to earlier timeframes.

54. Identity Theft Resource Center, *Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023*, STATISTA (Feb. 5, 2024), <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/> [https://perma.cc/Q2Q7-T4JF].

breach” because this study was designed to offer descriptive details specific to fact patterns that involve criminal behavior interrupting otherwise legal relationships that are usually premised on an uninterrupted chain of events. In contrast to studies involving more expansive terms, data breaches distinctly involve the unexpected and potentially unanticipated actions of a third party, which substantially change the nature of these cases, including harm analysis, standing, and the potential for future harm.

Another limitation involved the nature of the search tools. Westlaw is updated frequently, including the update of search algorithms and the cases provided to it from state and federal courts, with more federal court cases sourced. LexisNexis and Bloomberg Law could potentially offer different cases, but Westlaw is frequently used (and has previously been used on preceding empirical studies of data breach cases) for empirical studies, although it may be objectively incomplete. While PACER offers a complete view of federal cases, it does not provide state cases, limiting its utility. Google search also provides a heavily indexed list of sites, but it is not a definitive source of all information surrounding a data breach. However, it does provide some supporting information. Finally, given the limited nature of this study and the desire for a closed, tool-based system, the cases were not supplemented by attorneys representing plaintiffs or defendants.

Finally, the process of validating “data breach” cases to determine which cases involved a cyberattack fact pattern is a highly subjective decision. The research team validated these determinations, but the research lead made the final call for consistency.

D. *Corpus Overview*

Overall, the Westlaw search returned 456 cases, and 225 were determined to be bona fide “data breach” cases meeting study requirements.⁵⁵ Of the 225-case corpus, 172 were included in the

55. The goal of this research was to examine prevailing trends in data-breach litigation to inform potential legal interventions. Therefore, cases that did not reference the data breach or concern unrelated challenges (details of a motion to compel arbitration, for example) were maintained in an “out of scope,” separate corpus. About forty-nine percent of “data breach” cases met the criteria of data breaches involving an attacker compromising a technology system.

“complete” three-year data set.⁵⁶ In response to a Supreme Court case examining standing immediately following the planned conclusion of this study, *TransUnion LLC v. Ramirez*, an additional fifty-three cases were analyzed from 2020 to 2021 to extend the data set and to evaluate its effect on harm and standing analysis.⁵⁷

II. FINDINGS

This study confirms a number of findings from the Romanosky et al. study while also offering an updated and more detailed account of data breach litigation overall. The total number of “data breach” cases is lower than those found in the Romanosky et al. study likely due to methodological differences, but the average percentage of data breaches resulting in data breach litigation is similar. This study found a low of 0.2% of data breaches resulting in litigation in 2017, to a high of four percent of data breaches in 2020, illustrating a steady climb.⁵⁸ On average, 1.6% of data breaches have resulted in one or more cases for a breached defendant based on reported data breaches overall.⁵⁹ The four percent litigation rate is not substantially different from the litigation rate identified in the Romanosky et al. study, which identified a three percent rate nearing 2010.⁶⁰

56. Based on early analysis of case start and completion, three years appeared to include all case actions from the first case to the final case and became the lifecycle timeline for cases to end. Managing to a timeline ensured that all amendments, motions, and appeals would have concluded to ensure data fidelity.

57. 594 U.S. 413, 417 (2021).

58. See Romanosky et al., *supra* note 26, at 100 (estimating the federal-litigation-for-data-breach rate at four percent). This study narrows the number of cases by only using the term “data breach” for search, but it reflects a somewhat consistent ratio of federal litigation.

59. As described in the beginning of Part II, this frequency may be lower in earlier years due to a linguistic shift from “privacy breach” to “data breach.” See *infra* Section II.A. However, for purposes of this study, it was crucial to use the same linguistic search criteria rather than over-include non-bona-fide data breaches.

60. See Romanosky et al., *supra* note 26, at 85. If this data set was more similar to the breadth of the Romanosky et al. study, this rate might have been higher than four percent, illustrating a moderate increase in litigation frequency.

A. Cases and Circuit

The number of data breach cases has increased substantially from the first bona fide data breach case in 2005.⁶¹ Although the increase in cases is marked, it is possible that some differentiation is accounted for with a linguistic shift from “privacy breach” to “data breach,” or perhaps a shift from organizational mistake to cybersecurity incident as the basis for impact to personal information.⁶² Most likely, given the changing nature of cyberattacks and litigation generally, and after the highly publicized Target Corporation data breach cases,⁶³ 2013 was a critical turning point for data breach litigation.

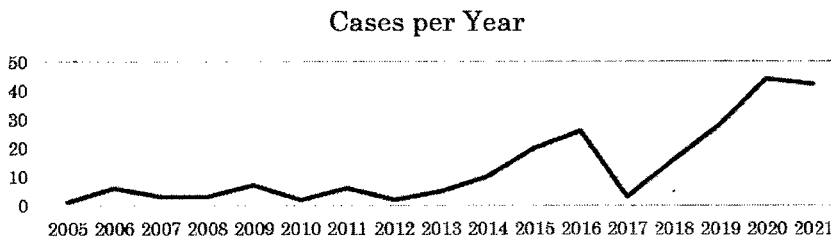


Figure 1: Data Breach Cases per Year

A significant majority of cases were brought in federal, rather than state, court. Only fourteen, a total of six percent, were heard in state court, refiled in state court, or heard in a combination of state and federal courts. Although this might appear at first glance as though most cases are filed in federal court—and this could be plausible based on diversity jurisdiction, especially for class actions—it may also mean that state cases are underreported to Westlaw.

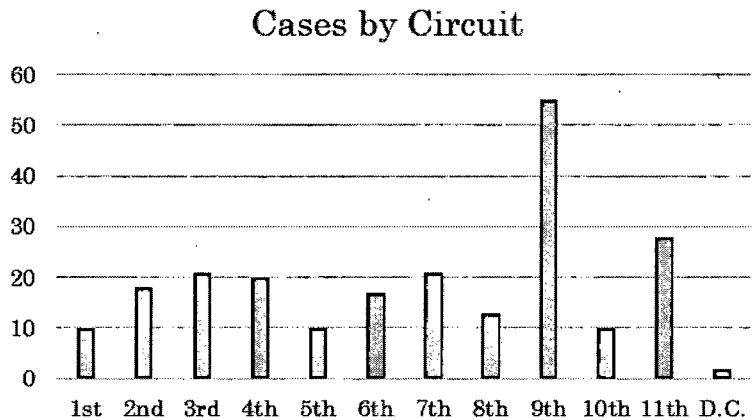
In federal court, a few circuits received more cases than others, but cases were heard in most circuits. The Ninth and Eleventh

61. *Infra* Figure 1.

62. As described in Romanosky et al.’s study, some data breach cases were dubbed “privacy breach” cases. Romanosky et al., *supra* note 26, at 79. However, privacy breaches can include a variety of other factual scenarios, including unauthorized disclosures and data mishandling, which do not involve a third party, intervening criminal act. *See id.* at 79 (referencing the various search criteria in addition to “data breach” that were used).

63. *See generally* Sciaroni v. Consumer (*In re* Target Corp. Customer Data Sec. Breach Litig.), 847 F.3d 608, 610–11 (8th Cir. 2017) (illustrating the consolidated class action lawsuit of Target customers against the company).

Circuits heard more cases overall than other circuits.⁶⁴ Despite cases being brought in all circuits, certain districts experienced more case frequency, with the top five state districts being California (twenty percent), Florida (eight percent), Illinois (eight percent), Pennsylvania (eight percent), and New York (six percent). Overall, data breach litigation is common across the United States.



*Figure 2: Data Breach Cases by Circuit (2005–2021)*⁶⁵

1. Case Timing and Disposition

Cases, on average, are heard on preliminary motions within 10.5 months of a data breach occurring. However, a small percentage of cases were filed later and heard up to five years after a data breach occurred. Despite plaintiffs filing complaints relatively quickly across examined years, cases varied in their average timeline to completion, with cases taking longer to conclude in more cases. From 2005 to 2011, cases took on average less than six months to conclude, while from 2012 to 2020, cases lasted around a year. Some cases were filed almost immediately after a data breach—sixty-two percent of complaints were filed in a year or less, and

64. See *infra* Figure 2.

65. For calculations using the entire data breach corpus, when courts heard these cases will be noted (including those brought in 2021). For calculations using the complete corpus (three-year lifecycle), the latest any cases will be noted is 2020. Data will be framed as to when it occurred—for example, a case could end in 2019, but it could have begun in 2018. Claims, then, would be attributed to 2018, while case decisions would be noted as 2019.

eighty-seven percent within two years.⁶⁶ This seems to suggest that defendants should expect litigation to commence within a year, if not sooner.

Consistent with the Romanosky et al. study,⁶⁷ eighty-five percent of these federal cases were plaintiff-defined as class-action lawsuits.⁶⁸ While additional cases that are not class actions have emerged at a greater volume in recent years, class-action lawsuits (usually from consumers) dominate the data breach litigation landscape.⁶⁹

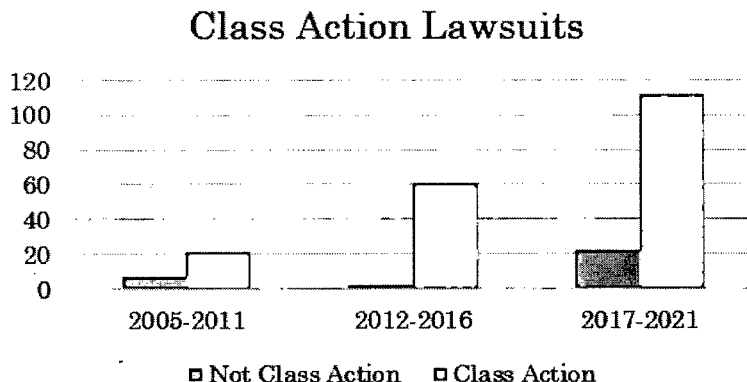


Figure 3: Class Action Lawsuits

2. Plaintiff Types and Data Types

Plaintiffs represented a variety of different positions with respect to defendants, with most plaintiffs being consumers (forty-four percent). However, a variety of other plaintiff types were represented, including patients (eleven percent), employees (eleven percent), and business customers (eleven percent).⁷⁰

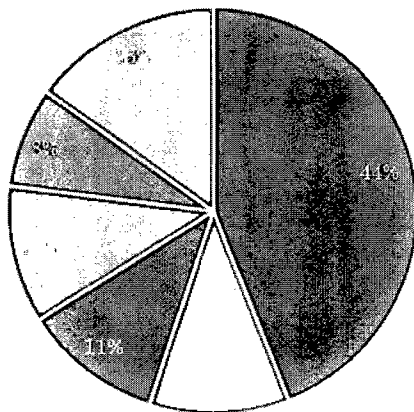
66. This seems to suggest that although there is a possibility of filing after two years, it is fairly rare.

67. See Romanosky et al., *supra* note 26, at 76.

68. It is important to note that class-action lawsuits continue to face substantial challenges in certification. See, e.g., Sciaroni, 847 F.3d at 612. It is difficult to determine whether all of these cases would or would not have been certified at this point in trial.

69. *Infra* Figure 3. It should be noted that these numbers may be influenced by states not reporting their cases to Westlaw or other search tools.

70. See *infra* Figure 4.



■ Consumer ■ Employees ■ Business ■ Patients ■ Banks/Trustees ■ Other

Figure 4: Plaintiff Types

Personal information compromised in the data breach giving rise to data breach litigation mostly consisted of highly sensitive categories of data, like payment card data, financial data, health data, and other sensitive data (a total of ninety-five percent).⁷¹ In far fewer cases, more general personal data like e-mail addresses or names were compromised (five percent). This seems to suggest that either (1) sensitive data compromised had potentially more value to an attacker, resulting in potential for harm (financial or otherwise), or (2) cases were more likely to be brought when sensitive data was compromised.

The type of data compromised can influence the degree and likelihood of harm, informing damages calculations and potentially settlement. Consistent with perceptions of harm associated with more sensitive data, it is similarly possible that courts might be less likely to find standing where data compromise does not involve sensitive data,⁷² influencing whether plaintiffs bring these cases or law firms take them. The frequency of intentional compromise may also demonstrate where this presumption could be wrong: where

71. *Supra* Figure 4.

72. *See* Lozada, *supra* note 9, at 475.

intentional compromise of seemingly innocuous data could be used to perpetuate greater harms or more complex attacks.⁷³

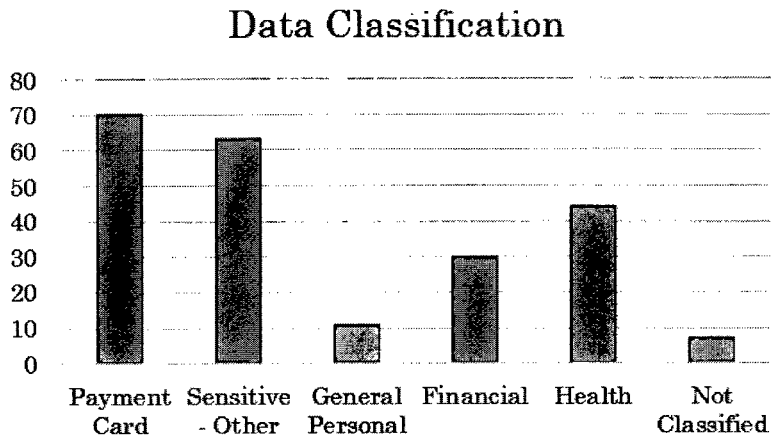


Figure 5: Data Classification of Litigation Subject Matter

Overall, most cases are class actions brought by consumer plaintiffs whose sensitive data has been compromised, which are brought within approximately twelve months of a breach, and conclude within approximately ten months after that. This seems to suggest that consumer cases conclude quickly, and that most cases have extended beyond pretrial motions. It also seems to suggest that the evidence available to these plaintiffs may be fairly limited at initial stages given the lengthy time to detect, contain, and investigate a data breach, often continuing after announcement.⁷⁴

73. It is well known in the cybersecurity community that, often, data are compromised as part of multi-step attacks, such as advanced persistent threat attacks, rather than simple and direct attacks. Therefore, it may be nearly impossible to determine, simply from the data compromised, whether future harm is likely to result.

74. Data breaches on average take about 277 days to detect and contain. See IBM, *Mean Time to Identify and Contain Data Breaches Worldwide from 2017 to 2024 (In Days)*, STATISTA (July 30, 2024), <https://www.statista.com/statistics/1417455/worldwide-data-breaches-identify-and-contain/> [<https://perma.cc/S2U4-QE87>]. Mean time to contain (after breach and potentially after data breach notification) is around seventy-three days alone. See *id.* However, the time to contain does not necessarily mean that all forensic investigations have concluded or that the organization has completed any necessary remediation efforts.

3. Procedural Position

Cases also conclude relatively early in the litigation process, with nearly zero cases making it past pretrial motions. A motion to dismiss was by far the most common end to cases, at sixty-seven percent of all cases, with a motion for summary judgment a distant five percent. Fifteen percent of cases overall were appealed, almost exclusively from a motion to dismiss and resolved in relation to those motions.

Only two of 172 cases have proceeded to trial. *Hiscox Insurance Co., v. Warden Grier, LLP* involved a data breach compromising sensitive and proprietary personal information maintained by Warden Grier on behalf of Hiscox Insurance Company but belonging to Hiscox and Hiscox's clients.⁷⁵ In 2016, The Dark Overlord, a hacking organization, compromised Warden Grier, and Hiscox only became aware of the breach after their data was posted on the dark web.⁷⁶ Ultimately, a jury rejected Hiscox's claims.⁷⁷ *In re Countrywide Financial Corp. Customer Data Security Breach Litigation* concerned the compromise of credit card information and proceeded to trial.⁷⁸ However, before the trial could proceed, a settlement was reached.⁷⁹

B. Standing

This study sought to identify key features of data breach liability cases, including how standing has evolved as a substantial

75. *Hiscox Ins. Co. v. Warden Grier, LLP*, No. 4:20-CV-00237, 2021 U.S. Dist. LEXIS 234765, at *1–2 (W.D. Mo. Dec. 8, 2021); see Kristin L. Bryan, Rafael M. Langer-Osuna & Ericka A. Johnson, *Key Litigation Takeaways from Rare Data Breach Trial*, NAT'L L. REV. (Apr. 4, 2022), <https://www.natlawreview.com/article/key-litigation-takeaways-rare-data-breach-trial> [<https://perma.cc/YB6H-TQTW>].

76. *Hiscox Ins. Co.*, 2021 U.S. Dist. LEXIS 234765, at *2; see Bryan et al., *supra* note 75.

77. Allison Holt Ryan, Adam A. Cooke, Lance Y. Murashige, Joseph J. Cavanaugh & Courtney E. Helt, *Data Breach Response Liability: Jury Finds Defendant Not Negligent for Response to Data Breach*, HOGAN LOVELLS (Apr. 19, 2022), <https://www.engage.hoganlovells.com/knowledgeservices/news/data-breach-response-liability-jury-finds-defendant-not-negligent-for-response-to-data-breach/> [<https://perma.cc/LF74-EYJW>].

78. See, e.g., *Sciaroni v. Consumer* (*In re Target Corp. Customer Data Sec. Breach Litig.*), 847 F.3d 608, 612 (8th Cir. 2017).

79. *In re Countrywide Financial Corp. Data Security Breach Litigation*, PRITZKER LEVINE LLP, <https://pritzkerlevine.com/case/in-re-countrywide-financial-corp-data-security-breach-litigation/> [<https://perma.cc/4ZDG-4L5K>].

impediment to data breach cases, which claims and harms theories garner outcomes in favor of plaintiffs, and whether and to what extent case law can help to explain what duties defendants may owe to plaintiffs. It is intended to offer descriptive information for plaintiffs, defendants, courts, and policy makers that may influence the overall development of a fragmented and largely under-developed area of the law.⁸⁰

Federal court standing requirements apply in federal cases and are based on Article III standing requirements. As established under multiple Supreme Court cases, a plaintiff must clearly specify harms constituting injury: (1) concrete and particularized actual injury or imminent injury-in-fact (cognizable and non-speculative),⁸¹ (2) the injury must be fairly traceable to the defendant's conduct (or omission), and (3) the injury must be able to be redressed.⁸² Standing challenges under 12(b)(1) question whether a plaintiff can bring a case based on claimed harms.⁸³

1. Background

Plaintiffs bringing cases following a data breach may have the most challenges satisfying the injury-in-fact requirement.⁸⁴ Cases where injury-in-fact is sufficiently specific to easily qualify under 12(b)(1) involve past harms that are direct⁸⁵—for example, an attacker steals and uses personal information to fraudulently charge someone's account or to release information resulting in loss of employment. Past harm may also be indirect. A third party may steal personal information, and although no direct harm from the criminal behavior immediately results, the plaintiff is harmed in other

80. This study will reference (and confirm) previous research on this topic within each area of discussion, where applicable.

81. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 n.1 (1992); *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339–40 (2016) (explaining that injuries must be “real” rather than “abstract”).

82. Martin H. Redish & Sopan Joshi, *Litigating Article III Standing: A Proposed Solution to the Serious (But Unrecognized) Separation of Powers Problem*, 162 U. PA. L. REV. 1373, 1375 (2014).

83. See FED. R. CIV. P. 12(b)(1).

84. Caroline C. Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 397 (2014).

85. *Id.* at 399.

ways: for example, by expending time and resources to avoid or mitigate future harm.⁸⁶

Alternatively, a plaintiff may argue that future harm may result from the third party's actions, such as enhanced risk of identity theft resulting from a past compromise.⁸⁷ Courts have tended to find standing more easily where past harms, or harms that have already occurred, are claimed, and where such harms are comparatively direct, or verifiable, with few exceptions. One primary exception for past and direct harm cases involves plaintiffs whose credit card issuers and banks have covered fraudulent charges.⁸⁸ Courts have become more skeptical of indirect past harm cases, specifically where a plaintiff's actions in avoiding harm are unreasonable concerning the potential harm (such as purchasing credit monitoring services when no other parties' personal information has been compromised).⁸⁹

Such harms may be considered injury-in-fact if intangible harms and even future risk of harm could be in "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit"⁹⁰ and injury-in-fact is actual or imminent.⁹¹ In 2007, the Government Accountability Office (GAO), for its part, studied the relationship between types of compromise and expected harms to examine the potential impact of data breach harms.⁹² Notably, the GAO remarked that "intentional acts . . . [are generally] considered

86. *Id.*; see Lozada, *supra* note 9, at 477–78.

87. See *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007) (noting that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions"); see also *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (identifying circuit split over whether increased risk of harm stemming from a data security breach constitutes an Article III injury).

88. See *Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89, 90–91 (2d Cir. 2017) (finding that fraudulent charges that were not paid by Whalen do not meet standing requirements); *c.f. Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966–67 (7th Cir. 2016) (citing *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690–91, 694 (7th Cir. 2015) (finding injuries sufficient for standing even when banks covered such fraudulent charges)).

89. Behnam Dayanim & Edward George, *Data Breach Litigation and Regulatory Enforcement: A Survey of Our Present and How to Prepare for the Future*, 1 CYBER SEC. 301, 308 (2018).

90. *Id.* at 303.

91. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013). For a complete examination of *Clapper* and its aftermath, see David W. Opderbeck, *Current Developments in Data Breach Litigation: Article III Standing After Clapper*, 67 S.C. L. REV. 599, 601–04, 607–08 (2016).

92. See Lozada, *supra* note 9, at 464–65, 464 n.23.

to pose more risk than accidental breaches.”⁹³ This seems to suggest that true data breaches involving intentional compromise potentially pose significant future risk to individuals affected, even if the injury has not already occurred.

Despite the fact that certain compromises may be associated with a higher likelihood of injury-in-fact or qualify as injury-in-fact, harm may be only a “highly attenuated chain of possibilities.”⁹⁴ Surprisingly, following *Clapper v. Amnesty International USA*⁹⁵ and *Spokeo, Inc. v. Robins*,⁹⁶ both cases concerning standing for federal claims,⁹⁷ courts in the Sixth, Seventh, Ninth, and District of Columbia Circuits began recognizing future harms as the basis for meeting 12(b)(1) challenges.⁹⁸ Conversely, early studies placed the Third, Fourth, and Eighth Circuits as comparatively more conservative in recognizing future harm status.⁹⁹

The 2021 *TransUnion LLC v. Ramirez* decision, however, added a dimension to claims of imminent future harm.¹⁰⁰ Specifically, the Second and Eleventh Circuits have adopted a more restrictive version of the more liberal position; namely, not finding future harm in recent data breach cases.¹⁰¹ In a recent decision, *McMorris v. Carlos Lopez & Associates, LLC*, the Second Circuit developed factors for assessing the likelihood of harm related to the nature of

93. *Id.* at 465 (alteration in original) (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 1, 6 (2007)).

94. *Id.* at 470 (quoting *Clapper*, 568 U.S. at 410).

95. See generally *Clapper*, 568 U.S. at 410 (exemplifying a court interpretation of standing for federal claims).

96. See generally *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339–40 (2016) (exemplifying a court interpretation of standing for federal claims).

97. Both *Clapper* and *Spokeo* surround the use of federal statutes, Section 702 of the Foreign Intelligence Surveillance Act and the Fair Credit Reporting Act, respectively: *Clapper* framed future harms as “certainly impending” with “substantial risk” of harm, and *Spokeo* reinforced the nature of the harm as “concrete,” which must be “de facto”—it must actually exist. Patrick J. Lorio, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 85–88 (2017); see also *Clapper*, 568 U.S. at 410; *Spokeo*, 578 U.S. at 339–40.

98. See Dayanim & George, *supra* note 89, at 304–05.

99. See Lorio, *supra* note 97, at 98–101.

100. See *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417; *id.* at 456–57 (Thomas, J., dissenting).

101. Avi Gesser & Johanna N. Skrzypczyk, *The Supreme Court TransUnion Case Part I—What It Means for Standing in Cyber Cases*, DEBEVOISE & PLIMPTON (July 8, 2021), <http://www.debevoise.com/insights/publications/2021/07/the-supreme-court-transunion-case-part-1> [https://perma.cc/VGF2-4UG2].

the disclosure itself.¹⁰² Although these decisions may appear relatively nuanced, for data breach litigation, they can be the difference between an examination of the complaint on its merits and finding for a defendant on a motion to dismiss based on 12(b)(1) without any discussion of the claims.

Although most standing challenges in Supreme Court cases concern 12(b)(1), 12(b)(6) challenges also apply to data breach litigation.¹⁰³ Under 12(b)(6), whether the plaintiff has plausibly established the *prima facie* case requirements for associated claims is dependent on whether the plaintiff has failed “to state a claim upon which relief [may] be granted.”¹⁰⁴ In standing challenges invoking 12(b)(6) under pretrial motions, such as a motion to dismiss, courts require plaintiffs to produce evidence to support their claims, but will “construe all evidence in the plaintiff’s favor.”¹⁰⁵ Ultimately, this means that standing cannot be fully litigated until trial, although many decisions made about standing occur in pretrial motions where limited evidence may be available to a plaintiff.¹⁰⁶

Although evidence may be construed in a light most favorable to the plaintiff, data breach details are largely confidential—and even the breached organization may not understand all details until a forensic investigation is complete.¹⁰⁷ Forensic investigations are

102. See *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021). These factors include:

(1) whether the plaintiffs’ data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

Id.

103. For purposes of examining injury-in-fact for meeting standing requirements, 12(b)(1) is the more powerful rule because “court[s] can pierce the pleadings,” examining broader evidence. Matt Sawchak, *Litigating Injury in a 75-1.1 Case: The 12(b)(1) vs. 12(b)(6) Distinction*, ELLIS & WINTERS: WHAT’S FAIR? BLOG (Mar. 24, 2015), <https://www.elliswinters.com/trade/litigating-injury-in-a-75-1-1-case-the-12b1-vs-12b6-distinction/> [<https://perma.cc/5K83-UZDA>]. However, 12(b)(6) concerns the broader claims of a plaintiff, as pleaded. See *id.* For this reason, a defendant may bring a motion to dismiss based on 12(b)(1) followed by a motion to dismiss based on 12(b)(6) if the initial motion was unsuccessful (and the plaintiff’s broader claims may not be substantiated).

104. FED. R. CIV. P. 12(b)(6); see *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56, 570 (2007).

105. Redish & Joshi, *supra* note 82, at 1377.

106. See 15 JAMES WM. MOORE, MOORE’S FEDERAL PRACTICE § 101.31 (3d ed. 2024).

107. See Chad Warner, *Cyber Attribution Difficulties, Risks, & Benefits*, MEDIUM (Mar. 7, 2022), <https://warnerchad.medium.com/cyber-attribution-difficulties-benefits-b757e693f9ce> [<https://perma.cc/4X5L-QKDC>] (explaining that publicly releasing the details of data

typically used by organizations to understand how the organization has been breached and to direct remediation efforts, which means they likely provide information that would be valuable to plaintiffs arguing that an organization has not performed their duty or obligation sufficiently to prevent the data breach.¹⁰⁸

Forensic investigations may take a long time to complete, they are maintained as highly confidential or products of attorney-client privilege,¹⁰⁹ and other proprietary information about the system in question and its vulnerabilities may be unavailable in pretrial motions. Therefore, plaintiffs are in a highly unfavorable position for purposes of providing any semblance of information sufficient to survive a 12(b)(6) motion to dismiss, even if they have sufficiently pled injury under 12(b)(1).¹¹⁰ Although courts in some cases are limiting privilege claims of defendants as they apply to forensic reports,¹¹¹ successfully obtaining access to forensic reports will only apply to discovery if a plaintiff survives pretrial motions.

Overall, standing has occupied considerable time and attention of courts in data breach cases. Motions to dismiss based on 12(b)(1) have received special attention by courts over time,¹¹² with comparably less attention spent examining 12(b)(6). This seems to

breaches may have adverse effects for national security such as “inform[ing] an attacker that they’ve been observed” and “mak[ing] future tracking and defense more difficult”). See generally *Timelines in Digital Forensic Investigation: From Investigation to Court*, FORENSIC FOCUS (Sept. 10, 2020), <https://www.forensicfocus.com/articles/timelines-in-digital-forensic-investigation-from-investigation-to-court/> [<https://perma.cc/VE5N-DRVR>] (describing the investigation process following a data breach).

108. Daniel Schwarcz, Josephine Wolff & Daniel W. Woods, *How Privilege Undermines Cybersecurity*, 36 HARV. J. L. & TECH. 421, 430, 450 (2023) (describing how attorneys often direct forensic investigators not to draft a report, when “the client had a particularly poor security posture”).

109. *Id.* at 455, 456 n.171, 457 (quoting an attorney calling pre-breach assessments “a plaintiff’s dream”). There may be other ways to access such information, such as where a plaintiff can demonstrate undue hardship, but this is generally in discovery rather than in pleadings and pretrial motions and may not be persuasive if other information and data are available to the plaintiff. See FED. R. CIV. P. 26(b)(3)(A)(i)–(ii).

110. Although courts may be required to construe facts in a light most favorable to plaintiffs in pretrial motions, plaintiffs still must have enough information to plausibly and cogently support their arguments in pleadings. C. Kevin Marshall, *Pleading Facts and Arguing Plausibility: Federal Pleading Standards a Year After Iqbal*, JONES DAY (June 16, 2010), <https://www.jonesday.com/en/insights/2010/06/pleading-facts-and-arguing-plausibility-federal-pleading-standards-a-year-after-iqbali> [<https://perma.cc/7W6X-AWB6>].

111. Matthew D. Krueger, Eileen R. Ridley, Aaron K. Tantleff & Jennifer L. Urban, Foley & Lardner LLP, *Maintaining Privilege Over Forensic Reports*, BLOOMBERG L. (Sept. 23, 2021), <https://aboutblaw.com/ZKt> [<https://perma.cc/BL3S-LFCX>].

112. See *supra* Section II.B.1 and accompanying notes.

suggest that courts, even after three standing cases in the Supreme Court within this data breach study's observable time period, continue to grapple with how to effectively examine standing in data breach cases. Although standing is far from settled for data breach cases, there has been some observable evolution in how courts analyze standing involving past and future harm status.

2. Standing and Harm Status: 12(b)(1)

Across the complete data set, plaintiffs claimed past harms (forty-six percent), future harms (forty-one percent), and blended aspects of both (thirteen percent).¹¹³ Claimed future harms became a far lower percentage of total cases from 2017 to 2021, at less than twenty-five percent of total cases. Likely, this illustrates hesitation in attorneys bringing future harm cases following the *Spokeo* standing case or a different strategy of recasting future harm as past harm.¹¹⁴ Although harm recasting or tying is a relatively new development post-*Spokeo*, it seems to have overcome some of the impediments of earlier future harm cases.

Across the complete three-year case lifecycle, defendants' 12(b)(1) motions to dismiss were not dominantly successful, even though future harm is a known and significant challenge for plaintiffs.¹¹⁵ Sixty percent of cases met 12(b)(1) requirements, while forty percent did not. This, to some degree, loosely mirrors harm status with forty-six percent of past harms and thirteen percent of cases that included a blend of harm statuses. In most cases, courts are looking for *some* evidence of past harm, even if in only a small portion of the class. When part of a class claims past harm, this logically generates a greater likelihood of future harm for other members of the class.¹¹⁶ However, the advantageous coupling of past and future harms for standing analysis may simultaneously create challenges for class certification unless other commonality

113. Some cases did not have a disposition noted.

114. See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339–340 (2016); John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J. L., SCI. & TECH. 943, 944–45, 968 (2016). The *Remijas* case offers some examples where future harm is less of an impediment to recovery. *Id.* at 944–45. As Biglow describes, the information hacked in *Remijas* was known with some particularity and some cards had been fraudulently charged already. *Id.* at 968.

115. See Biglow, *supra* note 114, at 944 (describing the circuit split in 2016 that has not yet resolved today).

116. See *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 690, 693 (7th Cir. 2015).

requirements are met.¹¹⁷ Most cases that did not survive defendants' 12(b)(1) standing motions to dismiss (and other pretrial motions) occurred in the interim time period before *Spokeo* was decided or as a reaction to *Clapper v. Amnesty International USA* (2013).¹¹⁸ Figure 6 illustrates the percentage of cases surviving 12(b)(6) challenges over time.¹¹⁹

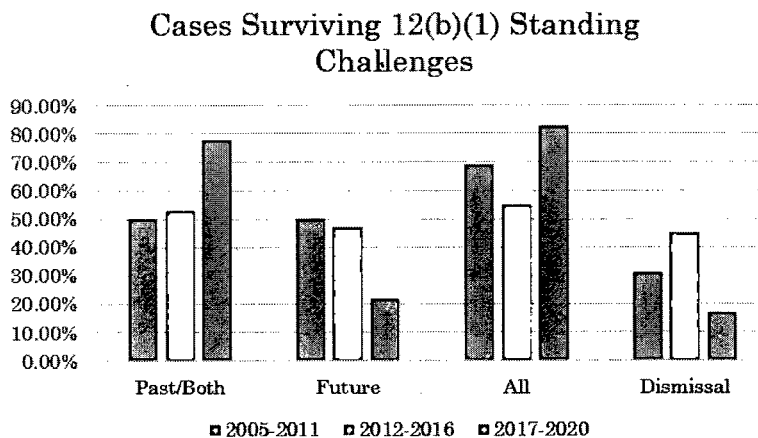


Figure 6: 12(b)(1) Challenges¹²⁰

Potentially, this reflects a reaction to the *Clapper* (2013) case restricting recognition of future harm as a basis for meeting 12(b)(1) standing requirements, which was more restrictive than previous years.¹²¹ The lower 2017 to 2020 percentage likely reflects parties bringing fewer cases claiming future harm after *Spokeo* (2016),¹²² self-selecting (either plaintiffs or their attorneys) based on a low likelihood of favorable outcome.

117. See discussion *supra* Section I.C.

118. See generally *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013). *Clapper* did not concern data breach litigation, but it likely affected the likelihood of plaintiff success from 2013–2016. *Does Clapper Silence Data Breach Litigation? A Two-Year Retrospective*, INFOLAWGRP. (Feb. 25, 2015), <https://www.infolawgroup.com/insights/2015/02/articles/breach-notice/does-clapper-silence-data-breach-litigation-a-two-year-retrospective#:~:text=This%20February%2026,%202015,%20marks%20the%20two-year%20anniversary%20of%20the%20> [https://perma.cc/72RD-UNQP].

119. *Infra* Figure 6.

120. Cases that survived 12(b)(1) dismissal may also include cases where the challenge was not raised.

121. See Danielle Keats Citron & Daniel Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 801–02 (2022); Kesan & Hayes, *supra* note 15, at 340; Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 447 (2017) (describing the *Clapper* decision as evidence of a growing movement in lower courts).

122. See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339–40 (2016).

Developing standing law may have shifted recognition of future harm to some extent, though perhaps not as significantly as expected. The Second (2009), Fifth (2007), Sixth (2006), and Seventh (2010) Circuits accepted plaintiffs' future harm arguments for standing in pretrial motions relatively early, and the First and Ninth Circuits recognized future harm in 2011, though most of the courts dismissed these cases anyway for failure to state a claim. One such case was *Rowe v. Unicare* (2010), a Seventh Circuit case involving the compromise of 210,982 insurance members' identification numbers, social security numbers, employment information, and medical information posted on a public website after Unicare failed to secure computer servers.¹²³ The plaintiff, Rowe, argued that the affected class members experienced anxiety and emotional distress.¹²⁴ The Northern District of Illinois' Eastern Division reasoned that "[g]iven the liberal pleading requirements of the federal courts" it would not determine whether Rowe's emotional distress was sufficiently severe for state law and Fair Credit Reporting Act claims.¹²⁵ Additionally, the court examined future risk of harm under both state and federal standards, finding that the possibility of future harm is not completely foreclosed.¹²⁶

In contrast with the early adopting circuits, the Eleventh and Fourth Circuits began recognizing future harm substantially later, in 2021 (the Eleventh, signaling a shift) and 2016 (the Fourth, in its first case). Overall, courts that recognized future harm before *Clapper* and *Spokeo* continued to recognize future harm, and other courts began to recognize future harm after these landmark decisions. The Third, Eighth, and Tenth Circuits have not recognized future harm as a basis for standing according to this study, and the DC Circuit has not heard a case involving future harm. It is possible that these outcomes can be explained by factual differences in the cases. However, it is unusual that not one in fifteen cases heard in these no-future-harm-circuits survived a 12(b)(1) challenge,

123. This failure may have exposed the data to hackers, but it was unknown at the time of the case whether any data had been actually compromised. See *Rowe v. Unicare Life & Health Ins. Co.*, No. 09-C-2286, 2010 U.S. Dist. LEXIS 1576, at *2, *23 (N.D. Ill. Jan. 5, 2010).

124. *Id.* at *10.

125. *Id.* at *13–14.

126. The court, adopting Illinois Supreme Court examinations of harm, reasoned that the principle of a single recovery creates a need to recognize future harm because "prohibiting recovery for future damages might result in an injustice to plaintiffs." *Id.* at *17–18.

suggesting an overall reticence to recognizing future harm as a basis for standing.

3. Theories of Harm and Damages

There are a variety of harm theories that have emerged in data breach litigation other than overt identity theft costs, such as costs to respond or manage the theft, and “cover” costs to prevent identify theft. These theories largely aim to reconceptualize future harm, or harms that have not yet occurred, as past harms. These theories accomplish this by connecting these harms to (1) the breach itself and (2) any underlying contractual bargain (whether implied or expressed).

Two theories of harm dominated data breach litigation: diminution of the value of PII and a lost benefit of the bargain.¹²⁷ Diminution of PII value is related to the objective value of PII on the open market, largely arguing that the loss of PII through data breach reduces its overall value economically.¹²⁸ Lost benefit of the bargain may adopt the traditional notion of contractual expectation damages as the basis for harm.¹²⁹ Or, plaintiffs may adopt a legal fiction of sorts—that they would have bargained differently if the bargain involved the compromise of their data (specifically, they would have paid less or forwent the bargain altogether).¹³⁰ This theory is related to the value of the transaction as a whole—the value of the transaction (e.g. service or goods) would have been lower if an individual was aware of the security characteristics (and attendant limitations) leading to the data breach. Because the value of the bargain would have been less, plaintiffs are theoretically owed the difference between what they actually paid and what they would have paid.

127. John DiGiacomo, *Data Breach Litigation: Theories of Damages in Data Breach Cases*, REVISION LEGAL (June 14, 2019), <https://revisionlegal.com/internet-law/data-breach/theories-of-damages-in-data-breach-cases/> [<https://perma.cc/D7DB-UWUL>].

128. *Id.*

129. *Id.*

130. *Id.*; Jim Dempsey, *US Courts Mixed on Letting Data Breach Suits Go Forward*, IAPP (Mar. 9, 2022), <https://iapp.org/news/a/u-s-courts-mixed-on-letting-data-breach-suits-go-forward/> [<https://perma.cc/J38N-APBP>]. It should be noted that although these may be argued as the basis for harm to meet standing requirements, they may also be used for purposes of calculating damages.

Within this data set, lost benefit of the bargain began as a harm theory in 2009 with *Cherny v. Emigrant Bank* and *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, both cases that would otherwise have claimed future harms as the basis of injury-in-fact.¹³¹ Neither case successfully argued this theory of harm. The first case successfully claiming this theory for future harm, at least partially claiming a win for plaintiffs, was *In re Sony Gaming Networks and Customer Data Security Breach Litigation* (2014).¹³² Although *Sony Gaming* did not proceed to trial, it was settled for \$15 million, with \$4 million towards identity theft monitoring.¹³³ This harm theory continues to be used in recent data breach cases: across the entire data set, the lost benefit of the bargain harm theory has been used thirty-three percent of the time, and this frequency is fairly consistent across time since 2012. In the full lifecycle corpus, parties that brought a benefit of the bargain harm theory were successful sixty-one percent of the time in surviving a 12(b)(1) motion to dismiss.

Diminution of PII was the dominant harm theory brought across the data set. The first successful case was *Rowe*.¹³⁴ Since this time, diminution of PII has become a more dominant theory, used forty-six percent of the time. Parties that brought a diminution harm theory were successful in surviving 12(b)(1) motions to dismiss about fifty-six percent of the time.

Of course, many plaintiffs have brought both theories of harm simultaneously to maximize the possibility of success; this occurred in twenty-two percent of cases. Of cases evaluated over a three-year period, about forty-seven percent of cases that cited both theories of harm were successful in surviving 12(b)(1) motions to dismiss. This seems to suggest that combining the diminution harm with the benefit of the bargain harm improves case outcomes where the facts support this.

131. *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 608 (S.D.N.Y. 2009); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 117–18 (D. Me. 2009).

132. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 2015 U.S. Dist. LEXIS 200092, at *19 (S.D. Cal. 2015).

133. See *id.*; Allison Grande, *Sony Gets Nod For \$15M Data Breach MDL Settlement*, LAW360 (July 11, 2014), <https://www.law360.com/articles/556813> [<https://perma.cc/2VB8-ER9C>].

134. See *Rowe v. Unicare Life & Health Ins. Co.*, No. 09-C-2286, 2010 U.S. Dist. LEXIS 1576, at *25 (N.D. Ill. Jan. 5, 2010).

4. Failure to State a Claim: 12(b)(6)

Although 12(b)(6) challenges to data breach cases have been largely undertheorized by academic researchers and not explored in much detail by courts, 12(b)(6), as a “failure to state a claim upon which relief can be given,” is far more connected to the substance of data breach cases.¹³⁵ Motions invoking 12(b)(6) examine to what extent plaintiffs have successfully pled their claims,¹³⁶ including which doctrines may impede their success.¹³⁷ For example, 12(b)(6) is typically invoked for the economic loss doctrine (“ELD”), which prevents plaintiffs from bringing tort claims when damages are only financial.¹³⁸

Although 12(b)(6) dismissals have historically been relatively low under the previous “no set of facts” standard,¹³⁹ across all cases in the three-year corpus, 12(b)(6) dismissals occurred in thirty-eight percent of total cases, which perhaps illustrates a post-*Twombly* higher pleading standard (and subsequent failure to meet such a standard).¹⁴⁰ Of the cases that did survive 12(b)(1) challenges, fifty-one percent did not survive subsequent 12(b)(6) challenges. Despite this, just over thirty percent of all cases survived both challenges, regardless of time period, and only around ten percent of future harm cases survived. Overall, this seems to suggest that thirty percent of cases would have proceeded to trial if they had not been settled, mostly cases involving past harm.

Some plaintiffs claiming future harm did survive motions to dismiss. For example, the *In re Capital One Consumer Data Security Breach Litigation* (2020) case involved the compromise of bank

135. See FED. R. CIV. P. 12(b)(6).

136. See Patricia W. Hatamyar, *The Tao of Pleading: Do Twombly and Iqbal Matter Empirically?*, 59 AM. U. L. REV. 553, 553 (2010).

137. *Twombly* (2007) heightened previous pleading standards, which included fair notice to the defendant and factual (but not legal) allegations accepted as true. *Id.* at 561, 563, 571. However, the U.S. Supreme Court, in a majority opinion by Justice Souter, added an additional requirement, “enough facts to state a claim to relief that is plausible on its face.” *Id.* This plausibility requirement does not create a probability requirement, but rather “it simply calls for enough fact[s] to raise a reasonable expectation that discovery will reveal evidence.” *Id.*

138. See Nicolas N. LaBranche, *The Economic Loss Doctrine & Data Breach Litigation: Applying the “Venerable Chestnut of Tort Law” in the Age of the Internet*, 62 B.C. L. REV. 1665, 1669 (2021).

139. See Hatamyar, *supra* note 136, at 574.

140. See *id.* at 582.

account numbers, credit scores, and a variety of other financial information of one hundred million customers. Capital One had stored this information on the Amazon Web Services Cloud, which had a “well-known vulnerability” involving a misconfigured firewall.¹⁴¹ The attacker publicly posted how to compromise the system using an SSRF attack on Github, Twitter, and Slack.¹⁴² Examining a variety of future harms recast as past harms, such as diminution of the value of their personal information, lost benefit of the bargain made with Capital One, mitigation expenses, and future risk of identity harm, the Eastern District of Virginia, Alexandria Division court examined 12(b)(6) for a variety of state law claims.¹⁴³

Applying Virginia law for some claims, which requires “probability rather than a merely possibility,” and “[d]rawing all inferences in favor of [the] [p]laintiffs,” the court held that the plaintiffs had plausibly alleged an actual fraud or risk of imminent fraud theory of damages.¹⁴⁴ Specifically, the actual compromise of some Capital One customers and the public nature of the hacker’s disclosure supported the probability of future misuse.¹⁴⁵ Overall, courts examining 12(b)(6) motions to dismiss and finding for plaintiffs may signal a shift towards examining data breach cases on the merits by applying state constructions of eligible harm.

C. Claims

Plaintiffs have brought a wide variety of claims, likely to increase the potential for success in a relatively new area of the law. In addition to 12(b)(1), courts have not always evaluated claims on the merits, usually because many courts have not meaningfully examined the case’s merits past the 12(b)(1) standing analysis in a motion to dismiss, which usually occurs first.¹⁴⁶ Likely because federal privacy laws do not broadly create a private right of action for data breaches (even though state laws have begun offering

141. *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F.Supp.3d 374, 388 (E.D. Va. 2020).

142. *Id.* at 389.

143. *Id.* at 390.

144. *Id.* at 402.

145. *Id.* at 402–03.

146. See Joseph F. Yenouskas & Levi W. Swank, *Emerging Legal Issues in Data Breach Class Actions*, 73 BUS. LAW. 475, 480 (2018).

these),¹⁴⁷ plaintiffs bring state law claims, including common law claims.¹⁴⁸ These claims included state consumer protection statutes, such as those provided by Unfair or Deceptive Trade Practices (UDTP) statutes, along with negligence and breach of contract claims, amongst others.¹⁴⁹

1. Claim Variation and Average Claims per Case

Plaintiffs have claimed a wide variety of potential causes of action. Plaintiffs brought claims based on state statutory bases, including UDTP and common law claims, as well as limited federal laws (or tort claims leveraging federal laws as the basis for establishing duty). Plaintiffs have claimed negligence, negligence per se, and less common torts involving trust, such as breaches of fiduciary duty and confidentiality, invasion of privacy, and even conspiracy and conversion. Plaintiffs also brought a wide variety of contracts claims: breach of contract, breach of implied contract, breach of bailment agreement, and breach of warranty. In addition, plaintiffs claimed tort-like contracts claims, such as breach of the implied covenant of good faith and fair dealing, unjust enrichment, misrepresentation, and fraud.

On average, plaintiffs brought cases most frequently for negligence, negligence per se, breach of contract, breach of implied contract, UDTP, and unjust enrichment.¹⁵⁰ State laws included UDTP, business confidentiality statutes, and data breach notification statutes that provide a private right of action.¹⁵¹

Strategies for claim articulation in pleadings have evolved over time, both the number of claims and the relative success of those claims. In the beginning, plaintiffs may have claimed more causes of action, as it was uncertain which claims could be successful, with

147. See, e.g., California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.150(a)(1) (2024); Illinois Biometric Information Privacy Act of 2008, 740 Ill. Comp. Stat. 14/20 (2024).

148. See Yenouskas & Swank, *supra* note 146, at 480–81.

149. *Id.* at 481–82. Many UDTP statutes include a private right of action. See Henry N. Butler & Joshua D. Wright, *Are State Consumer Protection Acts Really Little-FTC Acts?* 63 FLA. L. REV. 163, 166 (2011).

150. See *infra* Figure 7.

151. Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 71–72 (2015) (describing the availability of a private right of action in data breach notification statutes).

an average of 4.2 claims per case from 2005 to 2011.¹⁵² However, the average number of claims seems to have reduced as certain claims were not successful, falling to an average of 2.6 from 2012 to 2016. From 2017 to 2021, the average number of claims increased substantially to 6.5, buoyed by a variety of state law claims, such as multiple UDTP state laws across a class with private rights of action in large and very diverse class action lawsuits.

Over time, certain types of claims have become less popular: federal laws, breach of fiduciary duty, invasion of privacy, fraud, and breach of the implied covenant of good faith and fair dealing. Likely, these claims have reduced in frequency because of their unsuccessful results compared to other claim types.

2. Successful Claims

Some claim types have been more successful for plaintiffs than others. For the most part, the most common claims are also the most successful, with some limited variation. The most successful claim types based on this study are breach of implied contract (thirty-one percent) and negligence (twenty-eight percent). Several other claims were near this level of success: UDTP, breach of contract, unjust enrichment, and negligence per se.¹⁵³ The success of these claims is fairly consistent from 2012 to recent years.

152. In some cases, pro se plaintiffs simply described the conduct rather than specifying claims, consistent with reasonable acceptance of well-pled facts in pleadings. See Hatamyar, *supra* note 136, at 563.

153. See *infra* Figure 7.

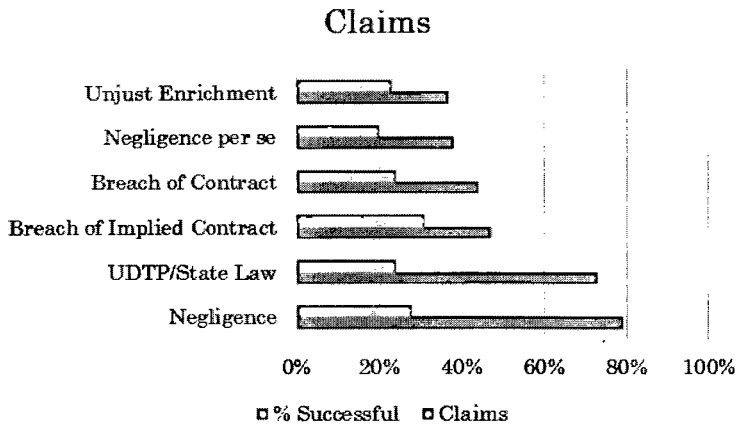


Figure 7: Claim Brought v. Plaintiff Success

3. Tort Law and the Economic Loss Doctrine

Because data breach litigation involves the intersection of privacy and cybersecurity law, a wide variety of torts could theoretically apply following a data breach. For example, invasion of privacy or intrusion upon seclusion,¹⁵⁴ privacy statutes with a private right of action,¹⁵⁵ negligence, and negligence per se claims could apply to a data breach depending on the facts.¹⁵⁶

In academic literature, negligence is the body of law most frequently examined in relation to data breaches.¹⁵⁷ Negligence applies to any set of facts where one party unintentionally inflicts harm on another party through their actions or omissions; that is, negligence organically can result from any relationship so long as the parties are connected by a causal chain of events.¹⁵⁸ Although individuals may be aware that they have provided personal information to an organization, they may not always know that their personal information has been shared with a third party for

154. RESTATEMENT (SECOND) OF TORTS §§ 652B, 652D (AM. L. INST. 1977).

155. See CAL. CIV. CODE § 1798.150 (West 2024).

156. See Tschider, *supra* note 18, at 130–31.

157. See Kesan & Hayes, *supra* note 15, at 317.

158. See *id.* at 318. As Kesan & Hayes acknowledge, *res ipsa loquitur*, a legal doctrine usually applied in products liability cases, could potentially apply to data breach cases. *Id.* Conceptually, it reasons that one party must be responsible for an injury because it could be no other—common in manufacturing defects where a consumer is harmed by the product. However, most causation is based on traditional but-for causation, supported by a factual inquiry at trial.

various reasons.¹⁵⁹ Tort law may be the only type of law that applies when individuals and organizations have no pre-existing relationship with each other (despite one party having custody of personal information).¹⁶⁰

A *prima facie* case for negligence requires: (1) the defendant breaches a reasonable duty of care; (2) the plaintiff suffers an injury-in-fact identifiable by the courts; and (3) the defendant's breach is the factual and proximate (legal) cause of the plaintiff's injury.¹⁶¹ There are at least three attendant challenges associated with these requirements. First, courts applying a specific state common law may not have historically recognized an injury-in-fact of the type claimed and may otherwise have great difficulty evaluating the harms claimed as meeting injury-in-fact standing requirements (whether established under the state or federal systems). For example, in *In re SuperValu, Inc.*, the Eighth Circuit reasoned that in Illinois, no affirmative duty exists to protect someone else from criminal activity, unless some special relationship applies, and the Illinois Supreme Court had not resolved whether a retailer (grocer) could have such a relationship with a customer.¹⁶² In *Community Bank of Trenton v. Schnuck Markets, Inc.*, the Seventh Circuit rejected a duty of data protection, characterizing it (based on a 2010 case) as a "new common law duty" to safeguard information.¹⁶³ The court further found that common law tort claims under Illinois and Missouri law should be dismissed based on a broadly construed ELD.¹⁶⁴

Second, courts may have great difficulty ascertaining what the reasonable duty for the defendant would have been at the time of

159. *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), <https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/> [<https://perma.cc/4VV5-GCNX>].

160. The existence of third parties, partners, data brokers, and many other business relationships often mean that these organizations do not always know that they are in any relationship with individual person. However, the existence of a data breach may trigger identification of the person for purposes of federal or state data breach notification statutes. This is in part because U.S. privacy laws do not typically require additional consent or even notification when personal information is shared with these organizations.

161. Kesan & Hayes, *supra* note 15, at 317.

162. See *Alleruzzo v. SuperValu, Inc. (In re SuperValu, Inc.)*, 925 F.3d 955, 963 (8th Cir. 2019).

163. *Cnty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 816 (2018) (quoting *Cooney v. Chi. Pub. Schs.*, 943 N.E.2d 23, 28–29 (Ill. App. 2010)).

164. See *id.* at 817–18.

breach.¹⁶⁵ For example, in *Deutsche Bank National Trust Co. v. Buck*, plaintiffs argued several distinct breaches of duty in both tort and contract.¹⁶⁶ Under Virginia's source-of-duty rule, courts must determine whether duty exists in tort or contract, which could not be identified, and Buck did not establish a contract or identify the basis of negligent conduct following a data breach.¹⁶⁷

Finally, courts may be challenged by the unique nature of the data breach's factual timeline and associated relationships between the parties in the causal chain.¹⁶⁸ One key challenge is the prevalence of simultaneous data breaches with different defendants but involving the same plaintiffs. The Eleventh Circuit in *Resnick v. AvMed, Inc.* noted that "[e]ven with . . . close connection in time . . . allegations only of time and sequence are not enough to establish causation."¹⁶⁹ However, in the *Resnick* case, the plaintiff took several careful steps that would eliminate the potential for multiple compromises, such as securely storing sensitive documents, securely destroying information, and not transmitting personal information in an unencrypted form, which made the plaintiff's arguments of the AvMed Inc. data breach causing identity theft more persuasive.¹⁷⁰

Because a compromising event, such as a cyberattack, is an intervening cause in the causal chain, the intervening cause must have been foreseeable by the defendant prior to the breach, and the defendant failed to exercise reasonable care to prevent it.¹⁷¹ Practically, it may be very difficult for plaintiffs to prove that the specific criminal behavior of a cyberattacker for this fact pattern was foreseeable from the perspective of an objectively reasonable defendant. However, courts may frame foreseeability within a sphere of behavior, a "general type of risk" that accompanies criminal behavior, as described by the Third Circuit.¹⁷²

165. See Tschider, *supra* note 18, at 143 (describing that torts are inherently relational and contextual).

166. *Deutsche Bank Nat'l Tr. Co. v. Buck*, No. 3:17-CV-833, 2019 U.S. Dist. LEXIS 54774, at *2 (E.D. Va. Mar. 29, 2019).

167. *Id.* at *7, *11–13.

168. See Kesan & Hayes, *supra* note 15, at 318.

169. *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2012).

170. *Id.* at 1326.

171. See Kesan & Hayes, *supra* note 15, at 318–19.

172. *Citizens Bank of Pa. v. Reimbursement Techs., Inc.*, 609 Fed. Appx. 88, 92 (2015).

Negligence per se may also be challenged by injury-in-fact and causation issues, though negligence per se is functionally different from negligence actions and might also introduce distinct issues. For one, negligence per se can apply under at least two circumstances. First, negligence per se establishes its duty of care from state or federal statute with a private right of action, though jurisdictions may differ in how the duty of care is established depending on the statutory language.¹⁷³ A clear negligence per se action arises when a statute has a private right of action that anticipates an intentionality of negligence (that is: not an intentional tort).¹⁷⁴ A statute with a private right of action will also include the basis for such a private right—specifically, express or implied statutory duties.¹⁷⁵ Negligence per se actions, then, inherit the basis for reasonable duty from statutory obligations rather than independent showing.¹⁷⁶ Following *Spokeo*, the existence of a statutory duty (and failure to perform it) does not alone satisfy the requirements for injury-in-fact for 12(b)(1) standing purposes.¹⁷⁷

Second, in some jurisdictions, negligence per se actions can use statutory obligations as the basis for duty, even if the statute does not permit a private right of action. For example, some jurisdictions allow plaintiffs to bring a negligence per se action for a data breach compromising health data using the security requirements established under the Health Insurance Portability and Accountability Act's ("HIPAA") Security Rule.¹⁷⁸ Although HIPAA does not have a private right of action, the primacy of HIPAA in the healthcare industry may nevertheless illustrate a common duty informed by statute in some states.

Breaches of reasonable or statutorily established duty may not always be recoverable, even if a plaintiff successfully argues

173. See RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 14 (AM. L. INST. 2010).

174. See *id.* cmt. a, b.

175. *Id.* cmt. b.

176. See *id.* cmt. b, c.

177. See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016).

178. EBIA, *Federal Court Dismisses Negligence Per Se Claim Based on HIPAA Privacy Rule Violation*, THOMSON REUTERS: TAX & ACCOUNTING (Apr. 28, 2022), tax.thomsonreuters.com/blog/federal-court-dismisses-negligence-per-se-claim-based-on-hipaa-privacy-rule-violation/ [https://perma.cc/6J7K-PBEY]. Courts may examine HIPAA and other federal laws without a private right of action as the basis for a negligence per se action differently, depending on the jurisdiction. For example, in *Walters v. Blue Cross & Blue Shield, Inc.*, the Northern District of Texas found that HIPAA could not a basis of a negligence per se claim. No. 3:21-CV-981-L, 2022 U.S. Dist. LEXIS 55061, at *15 (N.D. Tex. Mar. 28, 2022).

injury-in-fact and proximate causation. Under the ELD, economic harms may be barred from tort recovery.¹⁷⁹ As a doctrine applicable to tort law, the ELD reinforces the “stranger paradigm” principle, wherein courts are skeptical about unlimited liability to anyone and everything an organization could affect, especially when such liability does not involve physical injuries or damages to property.¹⁸⁰ Specifically, when two parties do not have a contractual or other special relationship, financial losses may be unforeseeable.¹⁸¹

A fairly large number of jurisdictions employ an alternative economic loss rule, specifically premising tort recovery on a special relationship between the parties, something “near-privity,” or an independent tort duty.¹⁸² A special relationship is established by examining factors but may involve relationships of trust (when one party relies on the other) or when one party is under the control of another (such as an employer/employee relationship).¹⁸³ Regarding an independent tort duty, this would presume that the state recognizes a tort duty akin to protecting personal information or provides a carve-out for negligent misrepresentation.¹⁸⁴

In addition to the stranger, unforeseeable liability problem, the ELD also aims to prevent the “two bites at the apple” or contracting-parties problem, meaning plaintiffs either seek the claim with the best economic recovery (typically tort, which permits punitive damages) or the claim with the most likelihood of success. The ELD did this by encouraging private ordering through contract.¹⁸⁵ Usually the ELD applies to sophisticated entities, such as businesses that have a contract or are otherwise within a contractual

179. LaBranche, *supra* note 138, at 1669.

180. See Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 348 (2017).

181. *Id.* at 348.

182. *Id.* at 354–55.

183. See *id.* at 366. Early cases for exceptions to the ELD based on special relationships involved six factors: (1) the defendant’s intent to harm the plaintiff, (2) harm foreseeability, (3) the certainty of a plaintiff’s injury, (4) the nexus between defendant’s actions and plaintiff’s injury, (5) moral blame of the defendant’s conduct, and (6) the objective of preventing future harm. *Id.* at 371–72 (describing *J’Aire Corp v. Gregory*, 598 P.2d 60, 63 (Cal. 1979)). Although these factors did not call out any preexisting relationships, existing relationships would likely result in satisfaction of more factors.

184. *Id.* at 355–56.

185. See *id.* at 361; LaBranche, *supra* note 138, at 1670. The ELD also limited the extension of liability to unforeseeable plaintiffs, specifically those in products liability who are “stranger[s].” LaBranche, *supra* note 138, at 1671–72.

relationship.¹⁸⁶ For this reason, it is expected that sophisticated entities include their obligations in the contract rather than attempting to recover under common law negligence. However, in some states, the ELD completely forecloses negligence actions before a plaintiff can argue such a case on the merits.¹⁸⁷ One exception to this is where plaintiffs can demonstrate a special relationship with the defendant. For example, in *Buckley v. Santander Consumer USA, Inc.*, the Western District of Washington recognized a special relationship between a business and its consumers to protect invitees from imminent criminal harm when third-party criminal conduct is reasonably foreseeable.¹⁸⁸

In this data set, plaintiffs relied to the greatest extent on tort law, especially negligence, though their success varied by circuit and by state common law.¹⁸⁹ This makes sense because businesses may not execute consumer contracts of adhesion that include how personal information will be protected. Therefore, tort law might be an alternative means of seeking recovery even where plaintiffs and defendants have a pre-existing contractual relationship.

In this study, negligence is the most frequently claimed: plaintiffs brought negligence actions seventy-nine percent and negligence per se actions thirty-eight percent of the time. Overall, these claim types were moderately successful given how frequently they were claimed.¹⁹⁰ Plaintiffs also brought breach of fiduciary duty

186. LaBranche, *supra* note 138, at 1676; see Sharkey, *supra* note 180, at 362 (“[T]here can be no recovery for purely economic losses when parties have had the opportunity to allocate risk according to the terms of their contractual relationship.”).

187. See Wajiha Rais & Lindy Stevens, *Economic Loss Doctrine*, A.B.A.: UNDER CONSTRUCTION (March 22, 2021), https://www.americanbar.org/groups/construction_industry/publications/under_construction/2021/spring2021/economic_loss_doctrine/ [https://perma.cc/NE8L-V997].

188. *Buckley v. Santander Consumer USA, Inc.*, 2018 U.S. Dist. LEXIS 53411 (W.D. Wash. 2018), at *13–14.

189. In the First Circuit, no negligence actions were successfully argued. In the Third and Fifth Circuits, very few negligence actions were successful. The Fourth and Eighth Circuits were moderately successful. Finally, the Second, Sixth, Seventh, Ninth, Tenth, and Eleventh Circuits were generally more favorable to negligence claims, with the Tenth and Eleventh better than fifty percent and the Sixth and Ninth at exactly fifty percent. The corpus numbers were relatively low; therefore, it is impossible to say definitively which circuits will be more amenable to tort claims, but it appears some circuits are generally more favorable, at least in preliminary motions. Negligence per se did not fare quite as well, although the Seventh and Eleventh Circuits appear to be most amenable to this type of claim. See generally *supra* Figure 7.

190. See *supra* Figure 7.

(twenty percent), invasion of privacy (twenty-four percent),¹⁹¹ misrepresentation (eighteen percent), fraud (seven percent), and false advertising (one percent) claims. Although scholars have explored trust-based relationships as the basis of information disclosure, courts have not recognized many of these claims.¹⁹² For example, plaintiffs claimed breach of fiduciary duty a relatively small percentage of the time, and the frequency of these claims has not increased over time, likely due to an overall lack of success (seven percent 2005 to 2011, four percent 2012 to 2016, and five percent 2017 to 2020).

One primary impediment to successful negligence claims is the ELD, which is not uniformly applied across all states. For some states, parties would have negotiated the terms of their engagement contractually, enabling plaintiffs to claim duties outside of their mutually assented agreement.¹⁹³ In other cases, states must identify a special relationship or independent tort duty to overcome the stranger paradigm, creating greater challenges for recovery when financial harm is claimed.¹⁹⁴ This is because most consumers

191. Invasion of privacy claims might have been brought a moderate amount, but generally these claims were not very successful, at only twelve percent, and falling out of favor from their peak in the 2005–2011 timeframe. See *supra* Figure 7. Overall, despite pretrial favorability to plaintiffs, this might be due to the intentionality requirement of most invasion of privacy claims, which would be difficult to demonstrate when the defendant is the organization that failed to protect personal information, not the entity compromising the data. Despite this, there have been arguments for a reinvigoration of invasion of privacy claims premised on a failure to intervene or inaction. See Jordan Elias, *Course Correction—Data Breach as Invasion of Privacy*, 69 BAYLOR L. REV. 574, 592 (2017).

192. See, e.g., Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559, 560 (2015) (describing the need for trust in personal information sharing); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 992–93 (2021) (describing the evolution of fiduciary duty from contractual to relationship-based); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492, 494 (2020).

193. For example, a consumer contract of adhesion, like a terms-of-use-agreement, might have already been executed, contractually governing the relationship between customer and business. Similarly, a contract could have been negotiated between two business entities. When a data breach occurs, typically the legal interests of both parties would have already been negotiated via the contracts governing their business relationships. If the harm is only financial, the ELD may apply and bar recovery for some torts. Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523, 528, 553–54 (2009).

194. It should be noted that this particular challenge creates a nearly insurmountable problem for plaintiffs strategically: if a plaintiff is likely to survive a 12(b)(1) standing challenge, they will likely have to claim financial harm. However, if they present financial harm as their injury-in-fact, they are likely to face an ELD bar that makes it much more difficult to recover for any tort claim.

would have assented to contracts of adhesion, which do not enable a true bargained-for exchange as would occur between sophisticated parties.¹⁹⁵

In this study, the ELD was explicitly mentioned in preliminary motions twenty-seven percent of the time, but its efficacy in foreclosing claims varied. The ELD, when raised, was effective forty-six percent of the time against negligence actions and twenty-six percent of the time against negligence per se actions. The difference in success can likely be explained by the difference between general duties under the negligence doctrine, which might be negotiated within a contract,¹⁹⁶ whereas negligence per se duties would be created by statute and potentially illustrate the creation of a special relationship or tort duty apart from general negligence (therefore making associated harms foreseeable).¹⁹⁷

Although negligence claims appear to be somewhat viable on pretrial motions, it should be noted that courts generally did not discuss prima facie case requirements associated with the claims, even claims that survived 12(b)(1) and 12(b)(6) motions to dismiss and met standing requirements. For example, very few courts meaningfully discussed reasonable duty. Without duty, a negligence claim cannot even begin to take shape—a duty that does not exist cannot be breached. Only seventeen percent of total cases examined duty in relation to negligence or contract claims.

For these cases, duty was established under a limited number of conditions. First, courts wrestled with whether duty fell under contract or tort. In one case, the court engaged in a “source of the duty” analysis to determine whether contractual duties applied.¹⁹⁸ In other cases, plaintiffs were not a party to the contract or may have been a third-party beneficiary that could not recover under a breach of contract action. Courts also examined whether

195. Andrew A. Schwartz, *Consumer Contract Exchanges and the Problem of Adhesion*, 28 YALE J. ON REG. 313, 347 (2011).

196. See Sharkey, *supra* note 180, at 378.

197. Certain circuits appear to be more amenable to plaintiffs surviving ELD defenses. The Fourth, Fifth, Sixth, Seventh, Eighth, Ninth, and Eleventh Circuits all permitted plaintiffs to bring negligence claims after the ELD was raised, which, at least for some cases, were successful in pre-trial motions. Overall, this seems to suggest that while the ELD is still a bar to some claims, it does not completely foreclose data breach negligence actions that otherwise survive 12(b)(1) and 12(b)(6).

198. *Deutsche Bank Nat'l Trust Co. v. Buck*, No. 3:17-CV-833, 2019 U.S. Dist. LEXIS 54774, at *7 (E.D. Va. Mar. 29, 2019).

misrepresentation had created an obligation to communicate about their security posture; for example, defendants are required to correct misstatements about their practices even if they are not required by law to disclose a data breach or security incident.¹⁹⁹

Courts wrestled with whether a common law duty to exercise reasonable care in storing and maintaining personal information even existed. On appeal, the Pennsylvania Supreme Court observed that establishing duty is dependent on the relationship of the parties, the social utility of the actor's conduct, the nature of risk imposed and foreseeability of harm incurred, the consequences of imposing a duty, and the overall public interest in a proposed solution, with the final factor dispositive for judicial efficiency.²⁰⁰

Other courts focused on a duty undertaken as a result of collecting and storing personal information. Duty may be established because a party undertakes a duty: if a defendant collects sensitive and private information from consumers and stores it on their network, they have a duty to protect it.²⁰¹ Although falling into the contractual framework rather than the torts framework, a handful of plaintiffs brought claims for breach of a bailment contract, premised on a similar theoretical framework—that defendants were accountable for holding responsibly in their custody the plaintiffs' data until they were no longer accountable for it. Surprisingly, this claim was successful in at least one case.²⁰²

In another case, duty was premised on a preexisting relationship where the defendant was required to protect its employees from foreseeable harm.²⁰³ Other courts defined that relationship as a

199. See *In re Marriott Int'l, Inc.*, 543 F. Supp. 3d 96, 111, 127, 134, 136 (D. Md. 2022).

200. *Dittman v. Univ. Pitt. Med. Ctr.*, 196 A.3d 1036, 1040 & n.2, 1042 (Pa. 2018) (quoting *Althaus ex rel. Althaus v. Cohen*, 756 A.2d 1166, 1169 (Pa. 2000)).

201. See *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1366 (S.D. Fla. 2015).

202. At least one of the eight cases bringing bailment claims were successful on those claims. *Bessemer Sys. Fed. Credit Union v. Fiserv Sols., LLC*, 472 F. Supp. 3d 142, 170–71 (W.D. Pa. 2020). But see *Galaria v. Nationwide Mut. Ins. Co.*, S.D. Ohio No. 2:13-CV-118, No. 2:13-CV-257, 2017 U.S. Dist. LEXIS 205304, at *8–9, *11–13 (Ohio Dec. 13, 2017). Miles Christian Skedsvold has proposed a data breach model that adopts the bailment lens to this end. Miles Christian Skedsvold, *A Duty to Safeguard: Data Breach Litigation Through a Quasi-Bailment Lens*, 25 J. INTELL. PROP. L. 201, 220–23 (2018) (observing that the duty of care implicit in a bailment agreement, whether express or implied, includes “safeguarding the bailor’s property”). Although typically bailment applies to tangible, moveable goods, Skedsvold adopts an approximation for data.

203. *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019).

special relationship that triggers an obligation to prevent a third party's wrongdoing.²⁰⁴ Most courts recognized duty premised on foreseeability. Some courts expressly observed that creating a "high degree of risk" triggered a finding of foreseeability and, following, a special duty to prevent injury-in-fact.²⁰⁵

Although defendants argued that the plaintiff did not establish a special duty related to their data, at least one court found that a general duty was enough.²⁰⁶ In another court, a breach of duty was found inferentially because the data breach occurred.²⁰⁷ Overall, state laws differ in terms of when a duty might exist, magnified by the complexity of data breach cases, including the foreseeable or unforeseeable unilateral actions of a third-party criminal in most cases.²⁰⁸

4. Contract Law

Both within sophisticated relationships and relationships between consumers and organizations, contract law may apply. In addition to the ELD's preference for private ordering, it may be easier to successfully claim breach of contract than successfully argue negligence. Four variations of contract law typically apply to facts in data breach cases: breach of express contract,²⁰⁹ breach of implied contract,²¹⁰ breach of the implied covenant of good faith and fair dealing,²¹¹ and breach of a bailment agreement.²¹² Although breach of the implied covenant of good faith and fair dealing is not a stand-alone claim, it may be used in addition to other breach of contract claims. Bailment agreements are typically argued in relation to goods but may be used in data breach cases

204. *Mackey v. Belden, Inc.*, No. 4:21-CV-00149, 2021 U.S. Dist. LEXIS 145000, at *22–25 (E.D. Mo. Aug. 3, 2021).

205. *In re Sonic Corp. Customer Data Sec. Breach Litig.*, N.D. Ohio No. 1:17-MD-2807, 2020 U.S. Dist. LEXIS 114891, at *7–10, *12–13 (July 1, 2020).

206. *Hapka v. CareCentrix, Inc.*, No. 16-2372, 2016 U.S. Dist. LEXIS 175346, at *12–13 (D. Kan. Dec. 19, 2016).

207. *Dittman v. Univ. Pitt. Med. Ctr.*, 196 A.3d 1036, 1048 (Pa. 2018).

208. *See Tschider*, *supra* note 18, at 117.

209. *RESTATEMENT (SECOND) OF CONTRACTS* §§ 235(2), 243(1)–(2), 245 (AM. L. INST. 1981).

210. *Id.* § 4 cmt. a.

211. *Id.* § 205.

212. Bailment agreements may be express or implied. *RESTATEMENT (FOURTH) OF PROP.* § 3 (AM. L. INST., Tentative Draft No. 3, 2022).

involving data custodians who are charged to maintain personal information on behalf of another entity.²¹³

The main claims under contract law include breach of express contract and breach of implied contract. Express contracts provide the entire basis for the terms of the relationship and typically involve the court's interpretation of any material term(s); the breach of the term(s) are the basis for the breach of contract action.²¹⁴ Under a breach of an express contract, the *prima facie* case requires the party claiming the breach to be in privity of contract (or sufficiently argue their status as entitled to some benefits of the contract as a third party), for the defendant to have breached a material term of the agreement, and for the plaintiff to have suffered some injury as a result.²¹⁵

In data breach cases, the terms of the agreement may not have contemplated the exact failure involved in the data breach, requiring courts to interpret terms that could include such failures, for example "reasonable security practices."²¹⁶ Although other documents, such as a privacy notice, could discuss security practices, they may be extrinsic to the agreement.²¹⁷ In many jurisdictions, courts may not interpret a privacy notice, provided on a website or web application, as the basis for an agreement or aggregated within another agreement.²¹⁸

Another crucial impediment to data breach cases involves binding arbitration provisions.²¹⁹ Courts may enforce binding

213. See Skedsvold, *supra* note 202, at 213–15 (noting that bailment theories themselves have largely been unsuccessful in data breach litigation involving personal information and suggesting that a quasi-bailment theory may be more successful).

214. See Ifeoma Ajunwa, *Genetic Testing Meets Big Data: Tort and Contract Law Issues*, 75 OHIO STATE L. J. 1225, 1257–58 (2014) (noting that genetic testing information—and perhaps broader privacy law—could fall “beneath a penumbra of property law, privacy law, and contract law”).

215. See RESTATEMENT (SECOND) OF CONTRS. §§ 235, 241 (AM. L. INST. 1981) (explaining that non-performance is a breach when performance is due and describing circumstances to determine when such a breach is material); see also *Hudson v. Wakefield*, 645 S.W.2d 427, 430–31 (Tex. 1983) (holding that the trial court should determine, as a matter of fact, whether a party's breach of contract is material).

216. See Tschider, *supra* note 18, at 100–01.

217. Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 911–12 (2016).

218. *Id.*

219. Stephen Jones, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis*, 50 TEX. TECH L. REV. 783, 785 (2018) (describing arbitration provision barriers to plaintiffs recovering in the *Equifax* cases).

arbitration and class action waivers in cases that involve breach of express contract claims, but these provisions may not be enforceable for other claims (e.g. torts, though some of these claims may be foreclosed by the ELD anyway).²²⁰ A recent data breach case, *Patrick v. Running Warehouse, LLC*, involved an arbitration provision located in a terms of use agreement that was linked near where an order is placed.²²¹ In this case, the Ninth Circuit found that inquiry notice of the terms of use agreement including the arbitration provision was enough to enforce the provision.²²² The existence of these provisions in largely consumer contracts can export a large volume of cases to binding arbitration, including mass arbitration.²²³

Courts have also recognized class waivers as the basis for defeating class certification in court.²²⁴ Although class waivers alone are not defenses to liability, they may prevent class action cases from going forward in the existing structure.²²⁵ In the event individual consumers bring data breach cases, they will not likely benefit from class representation, which largely extinguishes a great number of data breach cases that rely on collective injury claims (and potential for large settlements) to attract legal representation.²²⁶

220. Erin Jane Ilman & Alexis M. Buese, *Ninth Circuit Upholds Arbitration in Data Breach Case: A Reminder for Businesses on the Importance of Terms and Conditions*, NAT'L L. REV. (Feb. 28, 2024), <https://www.natlawreview.com/article/ninth-circuit-upholds-arbitration-data-breach-case-reminder-businesses-importance> [https://perma.cc/7Q8H-QLT8]; see LaBranche, *supra* note 138, at 1686.

221. *Patrick v. Running Warehouse, LLC*, 93 F.4th 468, 474–75 (9th Cir. 2024).

222. *Id.* at 477.

223. Ryan Phair, Carter Simpson, Emma Hutchinson & Hunter Nagai, *Federal Case Challenges Mass Arbitration “Shakedown” Amid Recent Amendments to AAA Rules*, PAUL HASTINGS (Feb. 16, 2024), <https://www.paulhastings.com/insights/client-alerts/federal-case-challenges-mass-arbitration-shakedown-amid-recent-amendments> [https://perma.cc/G2N6-964N]; Amir Alimehri, *The Table-Turning Risk of Mass Arbitration*, LOWEY DANNENBERG, P.C. (Mar. 30, 2020), <https://lowey.com/blog/the-table-turning-rise-of-mass-arbitration/> [https://perma.cc/4WP2-6VUS].

224. Amy Brown Doolittle, Katherine A. Spicer & Jay M. Thomas, *Recent Marriott Data Breach Class Action Decision Underscores the Importance of Class Action Waivers*, NAT'L L. REV. (Oct. 20, 2023), <https://www.natlawreview.com/article/recent-marriott-data-breach-class-action-decision-underscores-importance-class> [https://perma.cc/SU4R-TQM5].

225. These harms may be “small,” but large in the aggregate. Citron & Solove, *supra* note 121, at 816. Therefore, an individual harm might result in nominal damages, whereas a class would be substantially larger. See *id.*

226. *Id.* at 817.

In the event an express agreement does not exist, courts may find an alternative contract implied in fact.²²⁷ Implied contracts are contracts that exist not by evidence of mutual assent, as in a written agreement signed by the defendant, but rather evidence established by party behavior.²²⁸ For example, a party that provides access to an online service when another party provides their registration information could have formed a contractual relationship with them.²²⁹ Even if a terms of use agreement or similar contract does not alone manifest mutual assent, courts could observe the parties' performance, which evidences that some bargain has been struck and the parties mutually assented to it.²³⁰

Contract law claims comprise more than half of the most successful claims, including breach of contract, breach of implied contract, and unjust enrichment. This variation of claims reflects the specific facts of the case. For example, a breach of contract claim requires the existence of an agreement the law will enforce.²³¹ This would mean that any agreement would reference information handling obligations or security practices (and associated breach of their performance) leading to the data breach and resulting in harm to the plaintiff(s).²³² In other cases, when no express contract exists, a contract implied in fact may be created by observing the behavior of the parties, which illustrate mutual assent has

227. See Tschider, *supra* note 18, at 130.

228. *Id.*

229. Peter Karalis, *Analysis: Implied Contracts Add Legal Risk to Data Breach Cases*, BLOOMBERG L. (Aug. 19, 2021), <https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-implied-contracts-add-legal-risk-to-data-breach-cases> [<https://perma.cc/64YR-8ZEU>].

230. Contracts implied in fact may still require parties to demonstrate the same requirements as express agreements, which creates a more difficult standard for a party to demonstrate. See *Panther Brands, LLC v. United States*, 149 Fed. Cl. 204, 214 (Fed. Cl. 2019).

231. RESTATEMENT (SECOND) OF CONTRS. § 1 (AM. L. INST. 1981).

232. See *Deutsche Bank Nat'l Tr. Co. v. Buck*, No. 3:17-CV-833, 2019 U.S. Dist. LEXIS 54774, at *7 (E.D. Va. Mar. 29, 2019).

occurred absent oral or written agreement. Contract claim success varies based on the circuits in which they are brought.²³³

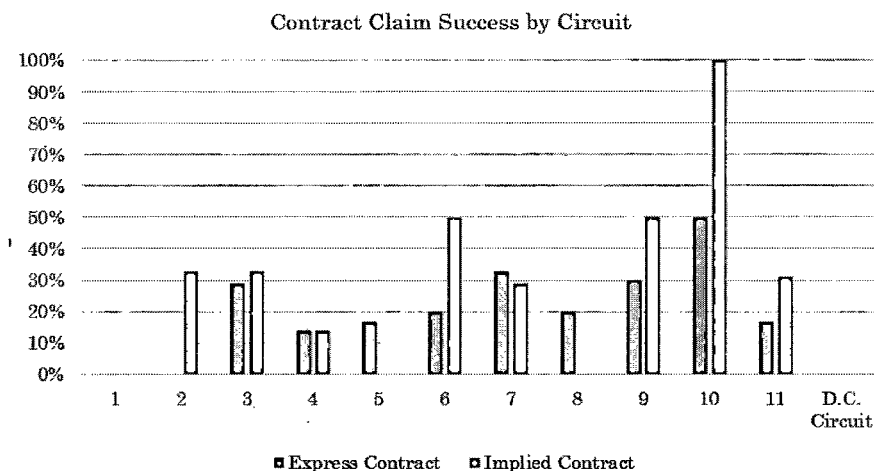


Figure 8: Contract Claim Type Success by Circuit

Nevertheless, parties may include some basis for determining the limits of that behavior. Plaintiffs have argued that a privacy notice should be enforced as a contract.²³⁴ In some jurisdictions, a privacy notice can form the basis of an express contract,²³⁵ though the absence of assent or acceptance by the plaintiff and the ability of the defendant to change the notice at their discretion usually results in courts not deeming it to be an express contract.²³⁶ In other cases, a privacy notice has been the basis of UDTP, misrepresentation, and fraud claims, as it accompanies an express contract and contains representations.²³⁷ A privacy notice can also be

233. State common law may differ in its receptiveness to successful breach of contract claims. The Ninth and Tenth Circuits are especially favorable to claims of breach of contract, and to some degree other circuits, with the exception of the First and Second Circuits, which did not accept any contract claims. Implied contract claims also vary significantly. The Second, Third, Sixth, Seventh, Ninth, Tenth, and Eleventh Circuits also seem favorable to breach of implied contract claims.

234. See Thomas Haley, *Illusory Privacy*, 98 IND. L. J. 75, 83 n.25 (2022). Privacy notices are typically considered “browse-wrap” terms, and their status as contracts has been hotly contested. *Id.* at 82. Discussion of privacy notice status as contract was “hotly” debated by the American Law Institute in relation to the Restatement of Contracts. *Id.* at 83.

235. Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45, 66–68 (2019).

236. See *id.* at 56, 65.

237. See *id.* at 57.

incorporated by reference, aggregated as part of a broader agreement and establishing express terms.²³⁸

Overall, plaintiffs referenced privacy notices thirty-two percent of the time and often when plaintiffs made breach of contract claims. The first case explicitly referencing a privacy notice was *Cherny*, where the notice accompanied claims of UDTP, breach of fiduciary duty, breach of contract, and misrepresentation.²³⁹ Although many contractual and representation-based claims could be brought when a privacy notice exists, certain claims are more explicitly tied to the existence of a privacy notice.

Plaintiffs leveraged the existence of a privacy notice for the following claims: a breach of the implied covenant of good faith and fair dealing (eighty-nine percent), breach of confidentiality (sixty-nine percent), breach of implied contract (sixty-five percent), breach of contract (sixty-four percent), and UDTP (sixty percent). Overall, the existence of a privacy notice could increase the probability of plaintiff recovery: fifty-five percent of cases citing a privacy notice resulted in a favorable plaintiff outcome. The presence of a privacy notice signals commitment from one entity usually to consumers, even if it is not explicitly part of an express contract and even if it does not include security obligations.

5. State and Federal Claims

In addition to traditional claims in tort and contract, many state laws permit plaintiffs to bring claims based on UDTP.²⁴⁰ UDTP statutes are loosely based on the Federal Trade Commission Act's Section 5, often dubbed "Little FTC" statutes, and require a demonstration that a defendant knowingly provided incorrect or false information or that the defendant was acting unfairly.²⁴¹ Unfair actions could include anticompetitive practices or failures in

238. See Haley, *supra* note 234, at 83–84.

239. *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 606–07 (S.D.N.Y. 2009).

240. Maggie Lynn McMichael, *Cybersecurity on My Mind: Protecting Georgia Consumers from Data Breaches*, 51 GA. L. REV. 265, 275–76 (2016).

241. Justin J. Hakala, *Follow-On State Actions Based on the FTC's Enforcement of Section 5*, U.S. FED. TRADE COMM'N 1, 2–3 (2008), https://www.ftc.gov/sites/default/files/documents/public_comments/section-5-workshop-537633-00002/537633-00002.pdf#:~:text=A%20Little%20FTC%20Act%20is%20a%20state%20act,righ%20of%20action%2C%20and%20FTC%20deference%2C%20vary%20widely [https://perma.cc/E3V9-58RX].

providing necessary information to plaintiffs; for example, information that would prevent incorrect assumptions.²⁴²

These claims may be brought by plaintiffs under a private right of action option associated with a UDTP statute.²⁴³ However, they could also be brought by a state attorney general.²⁴⁴ The foundation of UDTP could also inform nationwide multidistrict litigation, wherein multiple state attorneys general work in concert to bring a number of cases against a common defendant.²⁴⁵

One might imagine that without a firm common law basis for claims, plaintiffs might find alternatives in state and federal law claims. State claim frequency has grown substantially as multidistrict lawsuits and highly diverse classes have brought a wide variety of state law and UDTP claims. Across time periods, state claims were brought in seventy-three percent of cases, though only twenty-four percent, largely UDTP claims, were successful. Overall, the success of state law claims reached its peak in the 2012 to 2016 time frame, with a wider range of claims brought in the 2017 to 2021 time frame to comparatively less success.

242. Carmen D. Caruso, *A Fresh Look at State Little FTC Acts*, LITIG. COMMENT. & REV. (June 15, 2021), <https://litigationcommentary.org/2021/06/15/a-fresh-look-at-state-little-ftc-acts/#:~:text=To%20fill%20this%20void%2C%2049%20states%20have%20enacted%2C,lack%20of%20uniformity%20frequently%20creates%20outcome-determinative%20choice-of-law%20issues> [https://perma.cc/PXZ2-YXYD].

243. *Id.*

244. Martine E. Cicconi & Mark R. Herring, *State Attorneys General Flex New Muscle with Deceptive Trade Practices Laws*, REUTERS (Feb. 23, 2023), <https://www.reuters.com/legal/legalindustry/state-attorneys-general-flex-new-muscle-with-deceptive-trade-practices-laws-2023-02-23/> [https://perma.cc/XZ8B-4NGN].

245. *Id.*

Federal claims, while raised by plaintiffs, seem to be falling from preference because many of them have been unsuccessful.²⁴⁶ Federal claims have been brought in seventy of 225 cases (twenty-eight percent Fair Credit Reporting Act and twenty-five percent Federal Trade Commission Act), constituting thirty-one percent of the total corpus. These claims were only successful in three cases. When plaintiffs brought federal claims, often they claimed multiple statutes as the basis for those claims.²⁴⁷

Federal Statutes Claimed

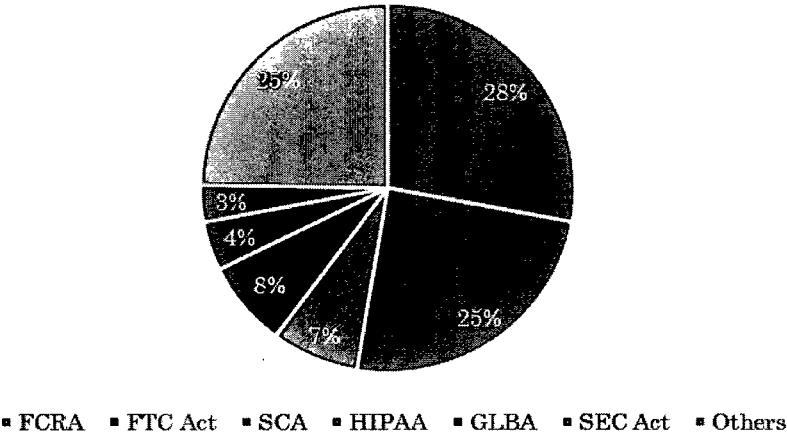


Figure 9: Federal Statutory Claims

Perhaps most interesting of federal statutory claims have been plaintiffs' use and subsequent court treatment of the FTC Act.²⁴⁸ The FTC Act does not create a private right of action; it only establishes what the FTC is required to do.²⁴⁹ However, the FTC Act also informs how states have worded their own UDTP statutes.²⁵⁰ In data breach lawsuits, the FTC Act may be used to inform the application of UDTP statutes or to establish expected duties in

246. This also seems to confirm Romanosky et al.'s observation that statutory support may not increase the probability of settlement. *See Romanosky et al., supra* note 26, at 98. After all, if the claim isn't legitimate based on the facts, it is not likely to garner much favor from the court.

247. *See infra* Figure 9 (providing a breakdown of the federal statutory basis of these claims).

248. The Federal Trade Commission Act of 1914, 15 U.S.C. § 45(a)(1).

249. *See Moore v. N.Y. Cotton Exch.*, 270 U.S. 593, 602–03 (1926).

250. *See Caruso, supra* note 242.

relation to contract or tort actions. For example, the Maine Supreme Court stated that FTC cases are not dispositive but could be instructive in data breach cases.²⁵¹ The First Circuit stated that the “host of FTC complaints and consent decrees condemning as ‘unfair conduct’ specific behavior similar to that charged by [the] plaintiffs” was not irrelevant.²⁵² Considering the frequency with which the FTC was invoked in data breach cases, the FTC may be influencing state UDTP application for data breach cases more than previously expected.²⁵³

6. Combined Claims

Although examined individually, plaintiffs regularly brought several claims simultaneously, perhaps strategically to see which claims might best fit a fact pattern. In this study, plaintiffs were often successful in claiming multiple claim types simultaneously (for example, contract, tort, and UDTP). These combinations do not necessarily illustrate a predictive trend of plaintiff claim behavior or relative success. However, courts may be permitting a number of claims to proceed in pretrial motions, even if such claims would not be successful at later trial. One reason may be that courts do not yet understand, like plaintiffs, which claims best fit typical data breach fact patterns. Additionally, because contracts and torts are largely relational, and UDTP statutes inform the relationship between businesses and consumers, these function as alternatives for each other, to some extent. Of the claim

251. *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492, 496 (Me. 2011).

252. *Amerifirst Bank v. TJX Cos. (In re TJX Cos. Retail Sec. Breach Litig.)*, 564 F.3d 489, 496 (1st Cir. 2009).

253. Scholars have debated the degree to which the FTC’s consent decrees mimic the common law. See Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014) (describing the role of the FTC with respect to administrative actions, mainly involving privacy activities); *c.f.* Justin (Gus) Hurwitz, *Data Security and the FTC’s UnCommon Law*, 101 IOWA L. REV. 955, 955 (2014) (describing the differences between administrative action and the common law, especially in relation to security rather than privacy actions). This seems to suggest that perhaps FTC consent decrees and analysis could affect the development of state common law and application of UDTP laws.

combinations most frequently deemed successful, the top five combinations included the following in Table 1.

Claim Combinations	Counts
UDAP/Negligence	19
UDAP/Negligence per se	17
Negligence/Implied Contract	16
UDAP/Implied Contract	15
UDAP/Express Contract	14

Table 1: Combined Claims Across Cases

7. Class Certification

A significant majority of data breach cases today involve class action lawsuits. Because class action lawsuits often involve diverse interactions with an entity, different contractual versions, or simply different harms (or disposition of harms), class certification may be difficult to satisfy in data breach cases.²⁵⁴ Few class challenges have been brought, and even fewer resulted in plaintiffs succeeding.²⁵⁵ In their most basic form, federal class certifications require the class meets the following requirements: (1) numerosity, (2) commonality, (3) typicality, and (4) adequacy of representation.²⁵⁶ The circuits may differ in their interpretation of these requirements.²⁵⁷

For data breach cases, class certification is inextricably intertwined with standing.²⁵⁸ If the class or members of the class have not suffered injury-in-fact meeting Article III, the class cannot be certified.²⁵⁹ In *TransUnion*, the Supreme Court held that every

254. Lyle Moran, *Data Breach Class Actions Are on the Rise, Report Finds*, LEGAL DIVE (Feb. 6, 2024), <https://www.legaldive.com/news/data-breach-class-actions-trends-class-action-report-duane-morris/706729/> [https://perma.cc/MG5B-VBHL].

255. Melissa Bilancini, *DSIR Deeper Dive: Class Certification Jurisprudence*, MONDAQ (July 7, 2022), <https://www.mondaq.com/unitedstates/data-protection/1207920/dsir-deeper-dive-class-certification-jurisprudence> [https://perma.cc/7TQT-KACQ].

256. FED. R. CIV. P. 23(b)(3), (c)(2)(B).

257. *Emerging Issues and Trends in Class Actions: Three Splits and Four Issues on the Horizon for 2024*, GIBSON DUNN (Dec. 28, 2023), <https://www.gibsondunn.com/emerging-issues-and-trends-in-class-actions-three-splits-and-four-issues-on-horizon-for-2024/> [https://perma.cc/A2Z7-AZZA].

258. *See id.*

259. *Id.*

class member must establish standing meeting Article III, though some circuits have permitted *de minimis* class members who have not suffered injury-in-fact to be included in the class.²⁶⁰ In the settlement context, injury-in-fact may also be required to permit settlement for all class members.²⁶¹ Moreover, for some courts, the injury-in-fact determination must be shared between class members to meet the commonality requirement (in addition to common fact pattern).²⁶² Ultimately, this means that courts may be evaluating or re-evaluating standing within class certification cases and not only motions to dismiss or motions for summary judgment.

Of special challenge is whether the type of claimed injury-in-fact is common between the plaintiffs.²⁶³ Plaintiffs suffering injury-in-fact could reasonably have suffered a different type of harm—some plaintiffs might have suffered identity theft, while others may only have suffered future risk of harm, complicating class certification based on commonality despite the same event causing these harms. Although the cases evaluated did not provide sufficient information to examine these challenges, they are likely to apply in many data breach cases.

8. Claims Overall

Overall, plaintiff status seemed to have a bearing on overall claim success. Unsurprisingly, plaintiff banks had the greatest likelihood, sixty-five percent, of surviving motions to dismiss with at least some claims, likely because business relationships would have resulted in execution of observable contract language. It is also more likely that these claims satisfied 12(b)(1) challenges because they involved concrete, past financial harms. Surprisingly, consumers and customers fared well on at least one claim, at fifty-nine and fifty-five percent, respectively. Although it might seem as if data breach cases are largely unsuccessful, at least in preliminary motions examined in a light most favorable to plaintiffs,

260. *Id.* (citing *TransUnion LLC v. Ramirez*, 594 U.S. 413, 427 (2021)).

261. *Id.*

262. *See, e.g., In re Marriot Int'l, Inc.*, 341 F.R.D. 128, 147–48 (D. Md. 2022) (describing common questions, practices, and technology infrastructure).

263. One key reason for bringing class actions is that individual harm may not be enough to substantiate litigation. Shay Lavie, *The Malleability of Collective Litigation*, 88 NOTRE DAME L. REV. 697, 705 (2012). However, amongst a class of different harms, there still must be some commonality to substantiate the claims. *Id.* at 722–24.

litigation is far from completely foreclosed. Of course, favorable plaintiff results in a motion to dismiss and other preliminary motions prompted settlement in many cases.

Notably, patients seemed to fare the worst of all plaintiff types, at only thirty percent successful cases on one or more claims. Although there may be multiple reasons for this outcome, some cases did use HIPAA as the statutory basis for negligence per se claims. Because HIPAA does not provide a private right of action, some states bar HIPAA (and similar statutes) as the basis for a negligence per se claim, which could have reduced plaintiff success.²⁶⁴

D. Settlement

As described in Part II, all but one case settled or concluded before trial because the plaintiff elected not to continue, or the court dismissed it. One common resolution of many cases, however, involved settlement. Across all time periods and case types, at least forty-three percent involved a documented settlement, while others may still be in the process of settling or settlement information could not be obtained.²⁶⁵ Settlement resulted when plaintiffs had a favorable outcome on the motion at issue before settlement (seventy-three percent),²⁶⁶ both parties had a favorable outcome on motions (forty-one percent), and occasionally even when the defendant had a favorable outcome (fourteen percent).

For purposes of this study, settlement amounts were calculated in relation to the number of impacted people (or organizations) according to the public disclosure either in court records or hosted on a public website.²⁶⁷ Unlike Romanosky et al.'s study, which

264. *E.g.*, *Walters v. Blue Cross & Blue Shield, Inc.*, No. 3:21-CV-981, 2022 U.S. Dist. LEXIS 55061, at *15 (N.D. Tex. 2022) (explaining that a statute without a private right of action cannot be used as the basis for a negligence per se claim).

265. Settlement was discovered using court documents on PACER and Westlaw, as well as Google searches to find both settlement end and settlement amount. It is acknowledged that settlement information may not have been available or may have been privately negotiated.

266. Notably, this percentage matches almost exactly Romanosky et al.'s estimate for when settlement is based on actual (i.e. past financial) harm. *See Romanosky et al.*, *supra* note 26, at 95–96. Favorable plaintiff outcomes in this study do include future and blended harm types, perhaps suggesting that courts are evolving on questions of harm as injury-in-fact.

267. This decision eliminated the need for determining the exact number of class members who did not opt out or were otherwise carved out of specific class action lawsuits. This

required contacting litigating attorneys to receive exact numbers of some settlement payments,²⁶⁸ this study approximated based on the size of the compromise and the total disclosed settlement. Although this does not provide an entirely accurate depiction of the settlement structure, it gives a broader sense of distinctions and differences between types of settlements.

The greatest frequency of settlement occurred with general personal information (fifty-seven percent) and with health data (fifty-five percent). However, the highest average settlement amount applied to payment card data, followed by health data and other sensitive data. Settlements ranged from \$0 to as much as \$600 per person. The average amount per person or organization was \$45.80, with a median value of \$2.20. This suggests that very large settlements increased the average, but most settlements were very low given the affected individuals.²⁶⁹ Some settlement amounts (per person or organization) were so low, the value was actually recorded as \$0.

Settlement/ Data Type	Low	High	Average	Median
Payment Card	0.03	600	57.13	2.4
Sensitive	0	86.5	19.6	2.7
Personal (non-sensitive)	0.02	0.13	0.08	0.08
Financial	0.11	40.2	14.5	3.5
Health	0	86.5	19.6	2.7
All	0	600	45.8	2.2

Table 2: Settlement Values/Data Type

activity was not completed to identify the *exact* settlement per person but rather to approximate the amount of settlement in relation to the size of the data breach, as well as factors that affect settlement.

268. *Id.* at 80.

269. *See infra* Table 2.

Settlement values appeared to drop for the most part in value per person as the number of affected people increased substantially.²⁷⁰

Affected People	Settlement Average/Record
1–5,000	228.60
5001–100,000	163.00
100,001–500,000	107.00
500,001–10 million	28.00
10–100 million	0.40
100 million +	1.10

Table 3: Settlement Average/Degree of Compromise²⁷¹

This table seems to suggest that most settlements “max out” at a smaller number of people because the settlement amount appears to be too high. Although some categories of affected people may have a limited number of cases informing the average, the table does paint a relatively clear picture of how data breach case settlements trend downward as the degree of compromise increases. Of course, settlement is up to the willingness of parties to negotiate and courts to accept proposed settlements.²⁷²

270. See *infra* Table 3.

271. It should be noted that these approximations are based on reported compromised records, not actual class members. Settlements included full settlement numbers where possible, inclusive of attorney fees, because some settlement disclosures did not specify attorney fees.

272. It should be noted that several bank settlements have been arranged for large numbers of reimbursement associated with covering fraudulent charges and reissuing cards. However, the number of banks affected for most of those settlements were comparatively small, as they banded together in smaller groups. For example, in the Target Corporation data breach litigation, the banks and card brands settled for \$19 million (Mastercard), \$67 million (Visa), and \$60 million for the rest of the class, with \$19.9 million in attorney’s fees. Memorandum and Order at 3, *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304 (2014) (No. 14-2522); *Target-Visa Settlement to Provide Up to \$67 Million for Card Issuers*, NATIONAL ASSOCIATION OF FEDERALLY-INSURED CREDIT UNIONS (Aug. 9, 2015), <https://www.nafcu.org/newsroom/target-visa-settlement-provide-67m-card-issuers> [https://perma.cc/ZY3Q-FJLT]; see *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1307 (8th Cir. 2014). Heartland Payment Systems was another breach that resulted in large payments to card brands: \$60 million (Visa), \$41.1 million (Mastercard), \$5 million (Discover). Proskauer Rose, *Heartland Payment Systems Enters into Its Third Settlement Agreement Arising from 2008 Data Breach*, PROSKAUER (May 24, 2010), <https://privacylaw.proskauer.com/2010/05/articles/data-breaches/heartland-payment-systems-enters-into-its-third-settlement-agreement-arising-from-2008-data-breach/> [https://perma.cc/6SRP-GQ83]; Linda McGlasson, *Heartland, Discover Settle for \$5 Million*, BANKINFO SEC.,

Settlement has been a hot topic amongst data breach scholars because typically a large portion is paid to law firms either for time and expenses (which can be substantial) or as a percentage-based fee.²⁷³ When settlement amounts for some class actions approach zero dollars and law firm payments constitute multiple millions of dollars, plaintiffs' advocate groups may wonder whether data breach litigation is accomplishing much for victim compensation. Moreover, unopposed settlements have been rejected by courts due to insufficient showing of standing, procedural issues, and perceived unfair attorney's fees.²⁷⁴

Settlements have, in limited cases (where disclosed), included security practices that organizations must implement. For example, eight organizations were required to provide credit monitoring services, three organizations must undergo annual professional assessments, and fourteen had to develop security programs and improve their security controls. Although these may not be exclusive to all settlements based on the information available, it provides a sense of additional measures that organizations must implement in addition to settlement costs.

<https://www.bankinfosecurity.com/heartland-discover-settle-for-5-million-a-2893> [https://perma.cc/F76Q-PY49]; see *Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 422 (5th Cir. 2013).

273. The Adobe class, from a breached database of 38 million users, paid their attorneys about \$1.1 million. Payout averaged \$0.03 per user. *In re Adobe Sys., Inc. Priv. Litig.*, 66 F. Supp. 3d 1197, 1206 (N.D. Cal. 2014); Order Granting Plaintiffs' Motion for Approval of Attorney Fees at 1, *In re Adobe Sys.*, 66 F. Supp. 3d 1197 (No. 13-CV-05226), ECF No. 107. The LinkedIn class, from a breached database of 6.4 million users, sought to pay their attorneys 32% of the settlement worth \$1.25 million, though the court awarded 25%. Payout averaged \$0.19 per user. See *In re LinkedIn User Priv. Litig.*, 309 F.R.D. 573, 581–82, 590–91 (N.D. Cal. 2015).

274. *Steven v. Carlos Lopez & Assocs., LLC*, 422 F. Supp. 3d 801, 803 (S.D.N.Y. 2019), *aff'd sub nom. McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d. Cir. 2021) (rejecting a settlement due to lack of standing despite no party objection to the settlement); Samantha Hawkins, *Filters Fast Data Breach Settlement Rejected over Notice, Fees*, BLOOMBERG L. (Feb. 16, 2022), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/XADM4T3S000000?bna_news_filter=privacy-and-data-security#jcite [https://perma.cc/V84L-248C] (discussing rejection of a settlement based on procedural issues, including “unfair” attorney’s fees); *Hymes v. Earl Enters. Holdings, Inc.*, No. 6:19-CV-644, 2021 U.S. Dist. LEXIS 26534, at *29–33 (M.D. Fla. 2021) (rejecting a settlement due to lack of standing, lack of specificity in administering the settlement, and insufficient notice specifications); *Hameed-Bolden v. Forever 21 Retail, Inc.*, No. 2:18-CV-03019, 2019 U.S. Dist. LEXIS 231593, at *29, *35 (C.D. Cal. 2019) (denying settlement based on inability to directly identify class members, insufficient notice specifications, non-identification of total settlement, and inability to evaluate attorney’s fees in relation to settlement).

III. FUTURE INQUIRY

This descriptive empirical study aims to provide additional information as a foundation for a more informed exploration of the future of data breach litigation. While clear conclusions from these data might be desirable, the presence of more modest indications tells a more interesting story. Despite evolution on a variety of fronts, courts are still in the process of developing this area of the law, after nearly two decades of exploration. Perhaps this result is a combination of factors: plaintiffs lacking the deep pockets needed to proceed and defendants attempting to settle quickly to avoid the unknown. Most importantly, perhaps the heavy focus on standing has prevented a more fulsome development of additional legal concepts, especially for the common law.

A. *Confirmations and Observations*

Despite being primarily descriptive in nature, this study also confirms previously empirically tested and observed information about data breach litigation. For example, the Romanosky et al. study continues to be applicable and correct in many respects despite the passage of more than a decade.²⁷⁵ While excellent scholars have tested and examined the law of data breaches, few have examined the details of litigation surrounding them.²⁷⁶

One observation is that, despite perceived challenges relating to standing, plaintiffs continue to bring data breach cases at a consistent rate with respect to the rising number of data breaches. The frequency of these cases has increased and does not show any sign of slowing down.²⁷⁷ Most of these cases are class-action lawsuits (or at least stylized this way),²⁷⁸ though class certification will continue to be an impediment as classes increase in diversity, as evidenced by the substantial uptick in state UDTP, privacy, and data breach notification laws referenced in these cases. Moreover, the

275. *Id.* at 74.

276. *See* Molitor et al., *supra* note 39, at 3–6.

277. *See id.* at 5–6.

278. *See* Romanosky et al., *supra* note 26, at 76.

type and status of harm (future, past, or a specific harm theory) may cause potential issues for class certification.²⁷⁹

Harm theories, especially the status of harm, will likely impact 12(b)(1) standing determination. Although future harm, or rather heightened risk of harm, is still an impediment to litigation,²⁸⁰ it is not completely foreclosed. Even though, at this time, it may be nearly impossible to claim harm based purely on emotional status, such as anxiety associated with the risk of harm,²⁸¹ plaintiffs have adopted creative solutions for recasting or tying more speculative harms to more concrete harms.

In one approach, plaintiffs expressly connect future risk of harm to past harms through diminution of value and lost benefit of the bargain harm theories. Another involves constructing a class action with two or more harm type sub-classes, with at least one risk of harm and another with past harm. Therefore, the premise of risk of harm is that it is likely to occur precisely because another subclass has actually suffered that harm from the same breach. Where possible, some plaintiffs brought a combination of past and future harms as a basis for their case.²⁸²

B. *New Contributions*

This study also provides new contributions on a variety of fronts, including significantly undertheorized areas primed for future exploration. Standing under 12(b)(6) enhanced pleading standards, the viability of various claim types, the influence of the FTC, settlement dynamics, and the future effect of credit monitoring offer many opportunities to influence future policy developments.

279. See, e.g., *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889–90 (11th Cir. 2023) (involving a class of plaintiffs with a similar harm of unauthorized payment card charges); *In re Marriott Int'l, Inc.*, 341 F.R.D. 128, 144 (2022) (showing that class certification is, in part, centered on the relationship between customers and Marriott, their hotel). In both cases, there was a substantial degree of diversity and associated state statutes, though they were able to certify despite this.

280. See *Citron & Solove*, *supra* note 121, at 817.

281. See *id.*

282. See *Romanosky et al.*, *supra* note 26, at 76.

1. 12(b)(6) Standing: A New Frontier

Although this study aimed to examine 12(b)(1) standing, 12(b)(1) standing challenges are not quite as dominant as previously thought. Sixty percent of cases survive a 12(b)(1) challenge, but they must still argue the merits of the claims they make.²⁸³ Defendants, therefore, have begun bringing 12(b)(6) standing motions,²⁸⁴ which will likely become another significant impediment for plaintiffs with post-*Twombly* and *Iqbal* plausibility pleading requirements.²⁸⁵ If courts engage with the claimed facts in a meaningful way, including examining what facts may simply not be possible to gather prior to discovery, plaintiffs could benefit. However, the challenge of plausibly pleading facts that may be absent from the public eye could also disproportionately favor defendants, the opposite of what flexible pleading requirements under the Federal Rules of Civil Procedure were originally designed to do.²⁸⁶

For defendants, bringing a 12(b)(6) motion may be a successful choice. Although defendants have frequently attempted to settle immediately after an unsuccessful 12(b)(1) motion to dismiss, it may make more sense for defendants to bring another motion based on 12(b)(6), as they have a reasonably strong chance of prevailing. This might not be fortuitous for plaintiffs, but courts actually hearing 12(b)(6)-based motions to dismiss could potentially enable exploration of injuries in relation to actual claims. This exploration would help resolve legal scholars' criticism that the 12(b)(1) standing inquiry has subsumed consideration of actual privacy torts.²⁸⁷ It might also enable the examination of harms in

283. See Citron & Solove, *supra* note 121, at 807.

284. See William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 234, 236–37, 239 (1988).

285. See A. Benjamin Spencer, *Understanding Pleading Doctrine*, 108 MICH. L. REV. 1, 4–5 (2009) (emphasis omitted) (footnote omitted) (describing a descriptive theory that defines contemporary pleading doctrine in relation to complaints that use “objective facts and supported implications . . . about which there is a presumption of impropriety”).

286. See Hatamyar, *supra* note 136, at 554–57. It is likely that construing 12(b)(6) in a light most favorable to the plaintiff to some degree began to degrade before *Twombly* and *Iqbal*, becoming more settled after these two Supreme Court cases. *Id.*; see also FED. R. CIV. P. 8(a)(2).

287. Indeed, modern standing law is a relatively recent concept, with most historical law directly examining the claims at hand. See Fletcher, *supra* note 284, at 224. As Felix Wu has argued, courts have embraced a wide variety of injuries to meet 12(b)(1), and the narrow application of it for intangible harms may be inconsistent with its precursors, which was still relatively limited. Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L.

relation to specific types of claims. For example, claims of immediate risk due to others suffering identity theft might not be compelling if the defendant paid for identity theft monitoring services; alternatively, in some courts the purchasing of identity theft monitoring services could demonstrate a higher risk of immediate harm.²⁸⁸

2. Claim Types and Court Preferences

Similar to standing challenges, the type of claims analyzed may also be different from those scholars routinely examine. Although negligence and negligence per se are dominant claim types, breach of express contract and breach of implied contract are nearly as significant, as well as UDTP claims. This demonstrates the openness of courts to recognize different factual articulations in the form of varying claims, or perhaps not exactly knowing which claim applies to the fact pattern for a data breach. Because the majority of cases ended in pretrial motions, it is hard to know which claims would have survived later at trial, especially because a large percentage of cases included multiple successful claims.

The viability of multiple claims for data breach fact patterns provides new avenues for considering the future of data breach litigation. Although scholars have examined negligence and other torts in relation to data breaches and other privacy incidents, far fewer have examined how breach of contract claims may or may not be viable and how that body of law may adapt to new environments.²⁸⁹

For example, although courts seek to uphold the contract to which parties have assented, courts have discretion in contracts

REV. 439, 442 (2017). Specifically, the focus was on the affected plaintiff, rather than the injury (effects) as a type of phenomenon. *Id.* at 446.

288. See, e.g., *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 788, 790–91 (W.D. Wis. 2019) (connecting purchasing credit monitoring services with defendant believing an increased risk applied to plaintiffs).

289. But see Tschider, *supra* note 18, at 99–100, 126–30, 145–46 (examining contract as a basis for data breach and other cyber incidents). Stacy-Ann Elvy has written extensively on this topic for Internet of Things products (i.e., household devices that are capable of automatically reordering goods), which include data storage and transmission, but not for intangible data specifically. See generally Elvy, *supra* note 217 (examining contract law, including the Restatement and the Uniform Commercial Code in relation to Internet-connected devices).

cases to interpret ambiguous terms.²⁹⁰ Under one of two theories—the business efficacy and the officious bystander tests—courts may also recognize implied terms,²⁹¹ such as an implied covenant of good faith and fair dealing (raised in the current study for ten percent of cases with a twenty-two percent success rate) or any other term that meets one of these theories and may have been omitted by the parties.²⁹² It is not hard to imagine how this could be important for ambiguous or open contracts of adhesion that heavily favor sophisticated entities.²⁹³

Additionally, plaintiffs bringing breach of contract claims following a data breach could include third-party claims. Third-party claims in contract might be successful when a data breach fact pattern involves a supply-chain attack. A supply-chain attack is an attack on third-party products, such as a web application a business uses, to compromise a different target—here, the defendant. Because the defendant has likely contracted with the business providing the compromised product, plaintiffs could potentially sue a business entity as a third party to their contract when they are injured by the breach, and the third party breached the contract.²⁹⁴ The advantage of bringing a claim as a third party to a contract is that a consumer or other plaintiff could benefit from the breach of contractual obligations between sophisticated entities so long as such claims are not disclaimed in another contract.²⁹⁵ This suggests that third-party claims (based on specific security requirements) could be an alternative to suing a defendant as a consumer

290. Under both Restatement- and UCC-based state laws, courts can either find ambiguity within the four corners of the completely integrated contract to permit introduction of parol evidence and explain ambiguity or courts may always introduce parol evidence under UCC-based laws. See Stephen F. Ross & Daniel Tranen, *The Modern Parol Evidence Rule and Its Implications for New Textualist Statutory Interpretation*, 87 GEO. L. REV. 195, 197, 205–06 (1998).

291. Steven W. Feldman, *Statutes and Rules of Law as Implied Contract Terms: The Divergent Approaches and a Proposed Solution*, 19 U. PA. J. BUS. L. 809, 830 (2017) (describing the court's challenge of not rewriting the contract, except for legal necessity).

292. Kathleen M. Miller, *When Can the Covenant of Good Faith and Fair Dealing Be Invoked?*, ABA BUS. L. TODAY (Feb. 22, 2024), <https://businesslawtoday.org/2024/02/when-can-the-covenant-of-good-faith-and-fair-dealing-be-invoked/> [<https://perma.cc/8CMK-L98T>].

293. In short, the lack of specificity in security language within contracts could give rise to the introduction of parol evidence, in particular industry practices, which provide some baseline of security practices.

294. But see *In re VTech Data Breach Litig.*, No. 15 CV 10889, 2017 U.S. Dist. LEXIS 103298, at *18–20 (N.D. Ill. July 5, 2017) (barring third parties from bringing third-party claims because their agreement with VTech disclaimed third-party beneficiaries).

295. But see *id.* at 28–29.

(especially where such claims are unlikely to succeed, such as against a governmental entity). For example, the defendant's vendor may not have appropriately installed an intrusion protection system on their network, despite such an action being required under the contract. While courts are generally skeptical of third-party claims in many cases, plaintiffs have not tried them extensively so far.

Contracts in general embody a variety of challenging dynamics that change the calculus of what duties may be owed, to what extent they may be owed, and when they will be performed. Unsophisticated parties like consumers are dependent on the expertise and expression of the defendant, and a lack of meaningful bargaining power will likely result in the application of contracts of adhesion.²⁹⁶ These contracts of adhesion—or “take it or leave it” contracts where one entity does not have the power to negotiate terms—are used regularly in sectors that have resulted in large data breaches and associated litigation, such as healthcare, insurance, employment, online services, and consumer products.

In other cases, when an express contract of adhesion, such as a terms of use agreement or other contract, does not exist, courts may find the performance of plaintiffs in providing information and defendants in providing a service based on that information as a contract implied in fact. In these cases, a robust examination of how underlying contracts doctrine should or can address these fact patterns is essential to future data breach litigation.

The overall claim landscape is evolving, which will require plaintiffs to evolve as well. Although it might be a useful exercise to propose or revive inventive claims, most plaintiffs today appear to be selective in their common law claims, focusing more heavily on statutory bases for recovery, at least where there is a private right of action. Despite academic interest in reviving niche torts,²⁹⁷ many

296. See Schwartz, *supra* note 195, at 348–49.

297. For example, Alicia Solow-Niederman makes an excellent argument for a revival of the breach of confidentiality. See generally Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. F. 614 (2018). However, typically this tort requires some special status, as Solow-Niederman identifies, a form of fiduciary duty. *Id.* Conceptually this might make sense, but common law limitations on confidentiality and fiduciary duty claims (for example, a narrow application of fiduciary duty under the common law, and typically an intentionality of disclosure requirement that may be hard to prove, even with a reckless intention) have made the claims

of these torts are lagging in frequency and attention, likely because (at least for data breach litigation) they have been much less successful. Similarly, federal claims are very unsuccessful and for this reason have fallen from favor in modern times despite their past popularity.

In addition to contract law, negligence continues to be an area where more attention is needed, specifically related to the mechanisms barring its claim and the prima facie case requirements. First, academics have noted the ELD's role in foreclosing negligence claims involving only financial losses.²⁹⁸ Surprisingly, the ELD in this study did not completely foreclose financial harm for at least two reasons: (1) many plaintiffs and defendants did not have the type of sophisticated relationship where a contract would be expected to allocate all obligations, and (2) most plaintiffs were consumers and other individual persons, largely dependent explicitly on the defendant to make reasonable discretionary decisions, which would not be specified in a contract if there were one. Importantly, courts specifically noted a "special relationship" exception to the ELD, which places certain cases outside the scope of the ELD.²⁹⁹ Since financial injury is likely to be claimed in data breach cases, at least for harms resulting from compromised virtual systems, further exploration into more expansive harm types and the associated limits of the ELD is necessary.³⁰⁰

Other than a focus on standing and the ELD, negligence and negligence per se's prima facie case requirements have received very little examination except in vague generalities. Initially, the preliminary matter of establishing a reasonable duty of care for

largely unsuccessful. In the present study, breaches of confidentiality were successful zero percent of the time, and breach of fiduciary duty was successful only six percent of the time.

298. See, e.g., David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 974 (2016) (describing how the ELD frustrates optimal economic dispersion of risk); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 300 (2005) (arguing that the protection of personal information defies typical bargained-for expectations in contract, citing data breach notification laws).

299. *J'Aire Corp. v. Gregory*, 598 P.2d 60, 63 (Cal. 1979); see Johnson, *supra* note 298, at 303 n.318 (quoting *J'Aire Corp.*, 598 P.2d at 63).

300. Plaintiffs framed most of the harms noted in the data breach cases as financial in nature. In that event, harms are explored more expansively, as recommended by Citron and Solove. See generally Citron & Solove, *supra* note 121, at 830–31 (describing a typology of different privacy harms that could be claimed in privacy lawsuits). As Citron and Solove note, a focus on pure economic loss is largely misplaced for lawsuits involving compromised privacy. *Id.* at 850–51.

data breach cases lacks a clear doctrinal approach.³⁰¹ Some theories explored by courts in this study incorporate a foreseeable risk of harm model, which is reinforced by data breach studies reporting that breaches usually result in stealing data or exposure of such data.³⁰²

This risk of harm model identifies a duty *because* risk of harm exists, rather than suggests that existing duties change with foreseeable harms. For example, a risk-of-harm-based duty might say that a defendant was obligated to remediate a system vulnerability because they became aware of the vulnerability, which posed risk to the plaintiff. However, courts may examine foreseeability of a preexisting duty differently: for example, the defendant owed a duty to reasonably protect data entrusted to them as part of their confidentiality obligations, but the performance of that duty is necessarily adaptive given foreseeable risk to the plaintiff. Yet another model might create a reciprocal duty: because one party has received data, it is obligated to reasonably protect it.

Each of these duty models presents a different analytical framing of negligence for courts. A foreseeable risk model would create narrow duties that are context-specific, rather than general. Under this model, the analysis focuses on how foreseeable the risk is. A preexisting duty model would be broad, illustrating why a defendant would have a positive duty, but tailored to the context of the situation. This model would likely involve examining the defendant's actions to determine if they are reasonable. In the reciprocal duty model, a court might examine what reasonable expectations might have accompanied the data provided—sensitive data might be encrypted, while non-sensitive data might only be password protected. Hypothetically, each could result in a different standard of care.

Negligence per se actions might also be challenging to evaluate from a duty perspective. Although they inherit duty from a statutory source, in some cases that statutory source might be federal or state statute with no corresponding private right of action, as is commonly the case for many federal privacy laws. Courts will then need to decide whether the duty is directly applied or otherwise

301. See Tschider, *supra* note 18, at 87.

302. Chlotia Posey Garrison & Matoteng Ncube, *A Longitudinal Analysis of Data Breaches*, 19 INFO. MGMT. COMPUT. SEC., 216, 219 (2011).

creates a standardized expectation of behavior that is highly persuasive. As observed in this study, some courts are willing to accept federal statutes like HIPAA and the FTC Act (both without private rights of action) as the basis for negligence actions, while others are not.³⁰³

In addition to these various examinations of duty, it is likely that courts would be challenged by the foreseeability analysis as it applies to the intervening criminal acts that disrupt and therefore complicate proximate causation analyses.³⁰⁴ It may also be tremendously difficult for plaintiffs to argue that certain injuries were “fairly traceable” from a defendant’s conduct that demonstrates a breach of reasonable or statutory duty.³⁰⁵ However, an undertheorized concept involves the use of *res ipsa loquitur*, which provides an alternative to more direct causation arguments by permitting a rebuttable presumption of negligence, for example, by framing proximate causation resulting in injury under the control of the defendant (or the defendant’s third-party supply chain) and unavoidable by a plaintiff.³⁰⁶ Although numerous co-occurring data breaches could reduce the viability of *res ipsa* as an alternative to traditional causation, it could be helpful in tort actions where the defendant is better able to avoid a cyberattack than the plaintiff.

3. The Influence of the Federal Trade Commission

Although this study found that federal claims have diminished over time, references to the FTC Act were prevalent through negligence, negligence per se, or UDTP claims. Overall, courts have seemed reasonably open to plaintiffs referencing FTC rationale or consent decrees in all of these claims.³⁰⁷ If the FTC’s guidance and enforcement (which are to some degree in limbo following

303. *In re Cmty. Health Sys., Inc.* No. 15-CV-222, 2017 U.S. Dist. LEXIS 21178, at *19 (N.D. Ala. Feb. 15, 2017); *supra* Section I.C.

304. See Tschider, *supra* note 18, at 81 n.22, 145.

305. *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1139–40 (C.D. Cal. 2021).

306. This is because *res ipsa loquitur* finds that injuries of a particular kind do not normally occur, so negligence is inferred. The coexistence of multiple simultaneously occurring data breaches could complicate this inference, but it could be available for some data breaches. See Kesan & Hayes, *supra* note 15, at 318 (examining duty and injuries for negligence actions).

307. *Supra* Section II.C.5. Although scholars have discussed the development of an FTC common law, scholars have not examined the impact of the FTC on the state common law.

*LabMD*³⁰⁸) will influence court analyses, perhaps the FTC will increase transparency in investigations and prioritize cybersecurity rulemaking.³⁰⁹

In addition, the frequency by which plaintiffs have cited privacy notices in this study likely merits exploration into how and to what extent privacy notices support a variety of claims. For example, privacy notices could establish some duty undertaken for negligence actions, implied or express terms for breach of contract, representations for purposes of misrepresentation/civil fraud, or evidence of unfairness in breach of the implied covenant of good faith and fair dealing. Although privacy notices may perform an important disclosive function absent any substantial, generally applicable privacy regulation,³¹⁰ it is unclear how and to what extent privacy notices that are provided by defendants to plaintiffs as a representation of their privacy practices should be evaluated in the context of a data breach case.

4. Settlement

As the number of data breaches have continued to increase, so has litigation.³¹¹ Some entities have suffered multiple data breaches. Despite a settlement rate (at least for documented settlements) of forty-three percent for cases without initially proving actual harm and seventy-one percent for cases with actual harm, this study illustrates that the larger the breach, the lower the settlement per person (approaching zero dollars), a trivial amount unless it satisfies some larger punitive goal.³¹² While large settlements could theoretically punish defendants to some extent (even when settlements do not include any admittance of fault), this study seems to suggest that large data breach settlements do not provide reasonable compensation, even when harms are

308. See *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1237 (11th Cir. 2018).

309. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2294–95 (2015) (describing limited disclosure of investigation).

310. M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1030–31 (2012). Of course, recent privacy law developments have expanded requirements beyond the privacy notice since 2012, but the privacy notice is still an important, legally mandated obligation.

311. See *supra* Section II.A.1 and accompanying notes.

312. See Romanosky et al., *supra* note 26, at 93–95 (finding a settlement rate around fifty percent); Citron & Solove, *supra* note 121, at 825.

aggregated in a class action lawsuit.³¹³ Although it may make sense to sacrifice some compensation goals to encourage deterrence through punishment,³¹⁴ the lack of court decisions (and associated jury awards) with useful direction on how organizations could improve their cybersecurity practices do not appear to accomplish deterrence or positive practices to avoid liability, either.

Ultimately, financial punishment in settlement could be too low, and the information accompanying punishment (such as which practices are normatively unacceptable and to what extent the defendant is at fault) is never disclosed. Alternatively, it is possible that data breaches are so inevitable that reasonably preventing well-resourced, high-aptitude attacks is nearly impossible.³¹⁵ While this fatalistic perspective is theoretically possible, many organizations fail to employ relatively simplistic security practices, too.³¹⁶ Therefore, scholars should at least explore whether increasing punishment or exposing failed practices could better result in deterrence.

There may be some options for encouraging a better outcome. As described in Part II, plaintiffs bring claims almost immediately and generally in less than a year from the data breach's occurrence.³¹⁷ Therefore, it may be worthwhile for plaintiffs to wait longer before commencing litigation and filing a complaint. While this could appear as if plaintiffs are artificially increasing their damages, waiting until sufficient information is available would enable plaintiffs to clearly articulate the factual basis for their pleadings, as well as their harms. Further, some documents that would be desirable in discovery may not be discoverable immediately following a data breach.³¹⁸

313. Citron & Solove, *supra* note 121, at 818–19.

314. *Id.* at 820–21.

315. Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. 172, 183 (2021).

316. *Id.* at 184.

317. See *supra* Section II.A.1.

318. See David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE-NOVO 151, 162 (2015); Brian Mund & Leonard Bailey, *Privilege in Data Breach Investigations*, 69 DEP'T JUST. J. FED. L. & PRAC., May 2021, at 39, 46–48; Schwarcz et al., *supra* note 108, at 426, 483 (describing extensively how attorneys may establish privilege to prevent the disclosure of post-breach forensic and other documents and recommending an alternative in favor of greater disclosure). Of course, this presumes three things: (1) plaintiffs are able to survive various pretrial motions, (2) the parties do not settle, and (3) documents regarding the cause of the breach would be discoverable in litigation.

For purposes of class organization in advance of certification, it would be prudent for plaintiffs to spend more time planning prior to bringing a lawsuit because more information could become publicly available about the breach, the attackers, how the system was compromised, and how the compromised data was used. Overall, this could improve available information concerning the causal link between the breach and data compromise (and whether the compromise creates substantial risk to the plaintiff).³¹⁹

5. Identity and Credit Monitoring

There are a variety of open questions related to harm that are not addressed in this study. This study did not examine the viability of identity and credit monitoring services as a mitigator for harm or a method for defendants to eliminate standing (preventing harm from occurring) by providing these services preemptively before litigation, nor did it feature prominently in any cases. Theoretically, purchasing these services, which may be required under some state laws,³²⁰ would reduce the likelihood of future harm. Unfortunately, there is no way of confirming this definitively unless the outputs of the services (thwarting identity theft) could be reviewed across a plaintiff class. Legally, we know very little about the nature of preventive monitoring and its effect on plaintiff and defendant's cases; is it a defense to a claim of harm under a negligence claim or admission of likely future harm speaking to foreseeability?³²¹ While these services were not explored in this study, they could affect future litigation.

CONCLUSION

This data breach litigation study has identified key trends and factors influencing case outcomes, examining the current state of data breach litigation. Principally, this study illuminates one of the most significant challenges: that courts have not yet developed a reasonably cohesive data breach common law. This lack of

319. See Citron & Solove, *supra* note 121, at 835.

320. Credit monitoring services can be required when highly sensitive data is compromised, specifically social security numbers. See, e.g., Assem. Bill 1710, 2013-2014 Reg. Sess., (Cal. 2014); CONN. GEN. STAT. § 36a-701b(b)(2)(B) (2025); DEL. CODE ANN. tit. 6, § 12B-102(e) (2025).

321. See Lozada, *supra* note 9, at 476-77.

cohesiveness has likely led to many cases with potential for plaintiff success settling before courts have an opportunity to meaningfully engage with the merits of each case. As theories of harm have evolved, so will arguments for a variety of claims as data breach cases are heard at trial. Courts have the unique opportunity to influence the development of an important and fast-growing body of law. Where there is a lack of established law, there is much opportunity for invention and creativity.

APPENDIX: CASE LIST

Case Name	Citation	First Case
Richardson v. DSW, Inc.	2005 WL 2978755	3-Nov-05
Banknorth v. BJ's Wholesale Club, Inc.	442 F.Supp.2d 206	13-Apr-06
Pennsylvania State Employees Credit Union v. Fifth Third Bank	2006 WL 1724574, 398 F.Supp.2d 317	16-Jun-06
Hendricks v. DSW Shoe Warehouse	444 F. Supp.2d 775	26-Jul-06
Giordano v. Wachovia Securities, LLC	2006 WL 2177036	31-Jul-06
Key v. DSW, Inc.	454 F.Supp.2d 684	27-Sep-06
Bell v. Acxiom Corporation	2006 WL 2850042	3-Oct-06
Pisciotta v. Old Nat. Bancorp	499 F.3d 629	23-Aug-07
<i>In re</i> TJX Companies Retail Sec. Breach Litigation (Financial Institutions)	564 F.3d 489	12-Oct-07
Ponder v. Pfizer, Inc.	522 F.Supp.2d 793	7-Nov-07
Sovereign Bank v. BJ's Wholesale Club, Inc.	533 F.3d 162	16-Jul-08
<i>In re</i> Countrywide Financial Corp. Customer Data Sec. Breach Litigation	588 F.Supp.2d 1368 (Mem)	23-Aug-08
Cherney v. Emigrant Bank	604 F.Supp.2d 605	12-Mar-09
Belle Chasse Automotive Care, Inc. v. Advanced Auto Parts, Inc.	2009 WL 799760 (Not Reported)	24-Mar-09
<i>In re</i> Hannaford Bros. Co. Customer Data Security Breach Litigation	4 A.3d 492	12-May-09
Lone Star Nat. Bank, N.A. v. Heartland Payment Systems, Inc.	729 F.3d 421	12-May-09
Wiley v. J.P. Morgan Chase, N.A.	2009 WL 1938987 (Not Reported)	7-Jul-09
<i>In re</i> TD Ameritrade Accountholder Litigation	266 F.R.D. 418	23-Oct-09
Amburgy v. Express Scripts, Inc.	671 F.Supp.2d 1046	23-Nov-09
CUMIS Insurance Society, Inc. v. BJ's Wholesale Club, Inc.	455 Mass. 458	11-Dec-09
Rowe v. Unicare	2010 WL 86391 (Not Reported)	5-Jan-10

Case Name	Citation	First Case
Allison v. Aetna, Inc.	2010 WL 3719243 (Not Reported)	9-Mar-10
Reilly v. Ceridian Corp. (denied cert)	664 F.3d 38	22-Feb-11
Resnick v. AvMed, Inc.	693 F.3d 1317	5-Apr-11
Claridge v. RockYou, Inc.	785 F.Supp.2d 855	11-Apr-11
Katz v. Pershing	672 F.3d 64	23-Aug-11
<i>In re</i> Michaels Stores Pin Pad Litigation	830 F.Supp.2d 518	23-Nov-11
Lone Star National Bank v. Heartland Payment Systems, Inc.	834 F.Supp.2d 566	11-Dec-11
<i>In re</i> Heartland Payment Systems, Inc. Customer Data Sec. Breach Litigation (Consumers)	2012 WL 896256 (Not Reported)	14-Mar-12
<i>In re</i> Sony Gaming Networks and Customer Data Sec. Breach Litigation	996 F.Supp.2d 942	11-Oct-12
Willingham v. Global Payments, Inc.	2013 WL 440702 (Not Reported)	5-Feb-13
<i>In re</i> LinkedIn User Privacy Litigation	932 F.Supp.2d 1089, 2014 WL 1323713 (Not Reported)	5-Mar-13
Bell v. Blizzard Entertainment, Inc.	2013 WL 12132044	11-Jul-13
Dieffenbach v. Barnes & Noble, Inc. (Formerly: <i>In re</i> Barnes & Noble Pin Pad Litigation)	887 F.3d 826	3-Sep-13
<i>In re</i> Zappos, Inc.	888 F.3d 1020	9-Sep-13
Galaria v. Nationwide Mutual Insurance Company	2017 WL 6375803	10-Feb-14
Strautins v. Trustwave Holdings, Inc.	27 F.Supp.3d 871	12-Mar-14
Citizens Bank of Pennsylvania v. Reimbursement Technologies, Inc.	609 Fed.Appx. 88	17-Jun-14
Moyer v. Michaels Stores, Inc.	2014 WL 3511500	14-Jul-14
<i>In re</i> Adobe Systems, Inc. Privacy Litigation	66 F.Supp.3d 1197	4-Sep-14
Burton v. MAPCO Exp., Inc.	47 F.Supp.3d 1279	12-Sep-14
Remijas v. Neiman Marcus Group, LLC	794 F.3d 688	16-Sep-14

Case Name	Citation	First Case
<i>In re</i> Target Corp. Customer Data Sec. Breach Litigation (Banks)	64 F.Supp.3d 1304	2-Dec-14
Doe v. Henry Ford Health System (cert. denied)	308 Mich.App. 592	18-Dec-14
<i>In re</i> Target Corp. Customer Data Sec. Breach Litigation (Customers)	66 F.Supp.3d 1154	18-Dec-14
Dolmage v. Combined Insurance Company of America	2017 WL 5178792	21-Jan-15
Peters v. St. Joseph Services Corp.	74 F.Supp.3d 847	11-Feb-15
Storm v. Paytime, Inc.	90 F.Supp.3d 359	13-Mar-15
Lewert v. P.F. Chang's China Bistro, Inc.	819 F.3d 963	27-Mar-15
Green v. eBay, Inc.	2015 WL 2066531 (Not Reported)	4-May-15
Vasquez v. Blue Cross of California	2015 WL 391674 (Not Reported)	5-May-15
Dittman v. UPMC	649 Pa. 496	28-May-15
Corona v. Sony Pictures Entertainment, Inc.	2015 WL 3916744 (Not Reported)	15-Jun-15
Wickens v. Blue Cross of California, Inc.	2015 WL 4255129 (Not Reported)	18-Jun-15
<i>In re</i> Ashley Madison Customer Data Security Breach Litigation (aka Avid Life Media) Consolidated complaint (total of 23 cases) MDL No. 2669	2016 WL 1366616 (Slip Copy)	22-Jul-15
Smilow v. Anthem Blue Cross Life and Health Insurance Co.	2015 WL 4778824 (Not Reported)	13-Aug-15
Abnale v. North Shore Long Island Jewish Health Systems, Inc.	49 Misc.3d 1027	14-Aug-15
Allen v. Schnuck Markets, Inc.	2016 WL 1427407 (Slip Copy)	27-Aug-15
Longenecker-Wells v. BeneCard Services Inc.	658 Fed.Appx. 659	22-Sep-15
McConnell v. Department of Labor	305 Ga. 812	12-Oct-15
Antman v. Uber Technologies, Inc.	98 Fed. R. Evid. Serv. 991	19-Oct-15
Weinberg v. Advanced Data Processing, Inc.	147 F.Supp.3d 1359	17-Nov-15
Walker v. Boston Medical Center Corp.	2017 - 34 Mass.L.Rptr. 387 2015 - 33 Mass.L.Rptr. 179	20-Nov-15

Case Name	Citation	First Case
Foster v. Essex Property Trust, Inc.	2015 WL 7566811 (Not Reported)	25-Nov-15
Whalen v. Michaels Stores, Inc.	689 Fed.Appx. 89	28-Dec-15
<i>In re</i> Supervalu, Inc.	925 F.3d 955	7-Jan-16
<i>In re</i> Anthem, Inc. Data Breach Litigation	2016 WL 3029783 (Slip copy)	14-Feb-16
Case v. Miami Beach Healthcare Group, Ltd.	166 F.Supp.3d 1315	26-Feb-16
Irwin v. Jimmy John's Franchise, LLC	175 F.Supp.3d 1064	29-Mar-16
Alonso v. Blue Sky Resorts, LLC	179 F.Supp.3d 857	14-Apr-16
<i>In re</i> Home Depot, Inc. Customer Data Security Breach Litigation (Banks)	2016 WL 2897520 (Slip Copy)	18-May-16
Khan v. Children's National Health System	188 F.Supp.3d 524	19-May-16
Chambliss v. Carefirst, Inc.	189 F.Supp.3d 564	27-May-16
Bradix v. Advance Stores Company	2016 WL 3617717 (Slip copy)	5-Jul-16
Duqum v. Scottrade, Inc.	868 F.3d 711	12-Jul-16
Torres v. Wendy's Company	2017 WL 8780453	15-Jul-16
<i>In re</i> Premera Blue Cross Customer Data Security Breach Litigation (Re-do)	198 F.Supp.3d 1183	1-Aug-16
Bohannan v. Innovak International, Inc.	318 F.R.D. 525	4-Aug-16
Attias v. CareFirst, Inc.	2021 WL 311000	10-Aug-16
Kaplan v. 21st Century Oncology Holdings, Inc.	214 F.Supp.3d 1357	10-Aug-16
<i>In re</i> Target Corporation Shareholder Derivative Litigation	Lead Case No. 14-cv-203 (PAM/JJK)	19-Aug-16
Unchageri v. Carefirst of Maryland, Inc.	2016 WL 8255012 (Slip copy)	23-Aug-16
<i>In re</i> The Home Depot, Inc., Customer Data Security Litigation	No. 1:14-md-02583-TWT	24-Aug-16
<i>In re</i> Community Health Systems, Inc. (motion denying appeal)	2016 WL 5409014 (Slip Copy)	12-Sep-16
Community Bank of Trenton v. Schnuck Markets, Inc.	887 F.3d 803	28-Sep-16

Case Name	Citation	First Case
Leibovic v. United Shore Mortgage, LLC	2016 WL 6395954	28-Oct-16
Welborn v. Internal Revenue Service	218 F.Supp.3d 64	2-Nov-16
Dugas v. Starwood Hotels & Resorts Worldwide, Inc.	2016 WL 6523428 (Slip copy)	3-Nov-16
<i>In re</i> The Home Depot, Inc. Shareholder Derivative Litigation	2016 WL 6995676 (Slip copy)	30-Nov-16
Hapka v. Carecentrix, Inc.	2016 WL 7336407 (Slip copy)	19-Dec-16
<i>In re</i> Experian Data Breach Litigation	2016 WL 7973595 (Slip copy)	29-Dec-16
Whitehead v. Advance Stores Company	2017 WL 2404922 (not reported)	9-Jan-17
Fero v. Excellus Health Plan, Inc.	502 F.Supp.3d 724	22-Feb-17
Stapleton on behalf of C.P. v. Tampa Bay Surgery Center, Inc.	2017 WL 3732102	30-Aug-17
Banus v. Whole Foods Market Group, Inc	2018 WL 549272	25-Jan-18
Provost v. Aptos, Inc.	2018 WL 1465766	12-Mar-18
Bray v. Gamestop Corporation	2018 WL 11226516	16-Mar-18
Patton v. Experian Data Corp.	2018 WL 6184772	28-Mar-18
Buckley v. Santander Consumer USA, Inc.	2018 WL 1532671	29-Mar-18
<i>In re</i> Sonic Corp. Customer Data Security Breach	2019 WL 3773737	17-Apr-18
<i>In re</i> Sonic Corp. Customer Data Security Breach	2021 WL 3269018	17-Apr-18
Moore v. HighPoint Solutions LLC	2018 WL 2684112	5-Jun-18
Scott Ables v. Brooks Brothers Group, Inc./ Brett v. Brooks Bros. Grp., Inc.	2018 WL 8806668	7-Jun-18
<i>In re</i> Equifax, Inc., Securities Litigation	357 F.Supp.3d 1189	18-Jun-18
Collins v. Athens Orthopedic Clinic Filed: 08/2018	849 S.E.2d 213	27-Jun-18
Gordon v. Chipotle Mexican Grill, Inc.	344 F.Supp.3d 1231	1-Aug-18
Pica v. Delta Air Lines, Inc.	2018 WL 5861362	18-Sep-18

Case Name	Citation	First Case
St. Paul Fire & Marine Insurance Company v. Rosen Millennium, Inc.	337 F.Supp.3d 1176	28-Sep-18
Bellwether Community Credit Union v. Chipotle Mexican Grill, Inc.	353 F.Supp.3d 1070	24-Oct-18
Tsao v. Captiva MVP Restaurant Partners, LLC Filed: 07/03/2018	986 F.3d 1332	1-Nov-18
Razuki v. Caliber Home Loans, Inc	2018 WL 6018361	15-Nov-18
Jackson v. Loews Hotels, Inc.	2019 WL 2619656	4-Jan-19
<i>In re</i> Equifax, Inc., Customer Data Security Breach Litigation	999 F.3d 1247	28-Jan-19
Ford v. [24]7.ai, Inc	812 Fed.Appx. 576	12-Feb-19
Arnold v. Anthem Inc.	2019 WL 1048254	5-Mar-19
McKenzie v. Allconnect, Inc	369 F.Supp.3d 810	28-Mar-19
Deutsche Bank National Trust Company as Trustee for Home Eq-	2019 WL 1440280	29-Mar-19
Huynh v. Quora, Inc. Filed: 12/2018	508 F.Supp.3d 633	11-Apr-19
McGarry v. Delta Air Lines, Inc. Filed: 11/2018	2019 WL 2558199	16-Apr-19
Sacklow v. Saks Incorporated	377 F.Supp.3d 870	6-May-19
Rudolph v. Hudson's Bay Company Filed: 09/2018	2019 WL 2023713	7-May-19
Fox v. Iowa Health System	2021 WL 826741	25-Jul-19
<i>In re</i> Brinker Data Incident Litigation (Green-Cooper v. Brinker International, Inc)	73 F.4th 883	1-Aug-19
Anderson v. Kimpton Hotel & Restaurant Group, LLC Filed: 04/2019	2019 WL 3753308	8-Aug-19
Thomas v. Kimpton Hotel & Restaurant Group, LLC Filed: 04/2019	2020 WL 3544984	8-Aug-19
Sabre GLBL, Inc. v. Kimpton Hotel & Restaurant Group, LLC	2021 WL 1839689	8-Aug-19
Hameed-Bolden v. Forever 21 Retail, Inc	2019 WL 8953127	12-Aug-19

Case Name	Citation	First Case
McGlenn (changed from Lavender) v. Driveline Retail Merchandising, Inc.	2019 WL 4237848	6-Sep-19
McGlenn v. Driveline Retail Merchandising, Inc.	2021 WL 4301476	6-Sep-19
Thomas v. Harry Filed: 05/2019	2020 WL 5110657	17-Sep-19
Fulton-Green v. Accolade, Inc.	2019 WL 4677954	24-Sep-19
Stephens v. Availity, L.L.C. Filed: 10/2019	2019 WL 13041330	1-Oct-19
Kimbriel v. ABB, Inc. Filed: 05/2019	2019 WL 4861168	1-Oct-19
Steven v. Carlos Lopez & Associates, LLC (McMorris v. Carlos Lopez) Filed: 07/2018	422 F.Supp.3d 801	22-Nov-19
Eades v. Wetzel Filed: 03/21/2019	841 Fed.Appx. 489	22-Nov-19
Adkins v. Facebook, Inc. (changed from Bass v. Facebook)	2021 WL 1817047, 424 F.Supp.3d 686, 2020 WL 6710086	26-Nov-19
City of Chicago v. Marriott International, Inc	626 F.Supp.3d 814	13-Dec-19
<i>In re</i> Dominion Dental Services USA, Inc. Data Breach Litigation	429 F.Supp.3d 190	19-Dec-19
Portier v. NEO Technology Solutions	2019 WL 7946103	31-Dec-19
Savidge v. Pharm-Save, Inc	2020 WL 265206	17-Jan-20
Heidbreder v. Epic Games, Inc. Filed: 08/2019	438 F.Supp.3d 591	3-Feb-20
<i>In re</i> Alphabet, Inc. Securities Litigation	1 F.4th 687	5-Feb-20
Bank of Louisiana v. Marriott International, Inc. Filed: 12/2018	438 F.Supp.3d 433	7-Feb-20
Paymentech, LLC et al v. Landry's Inc.	2021 WL 1856553	10-Feb-20
Guo Wengui v. Clark Hill, PLC Filed 10/2019	440 F.Supp.3d 30, 2021 WL 106417	20-Feb-20
Pruchnicki v. Envision Healthcare Corporation	845 Fed.Appx. 613	20-Feb-20

Case Name	Citation	First Case
<i>In re</i> Marriott International, Inc., Customer Data Security Breach Litigation (Multi-district litigation incl. consumers and Chicago govt)	543 F.Supp.3d 96, 341 F.R.D. 128, 112 Fed.R.Serv.3d 1299, 440 F.Supp.3d 447	21-Feb-20
Toretto v. Mediant Communications, Inc. Filed: 03/2020	2020 WL 1288478	18-Mar-20
Braun v. Mediant Communications, Inc. Filed: 10/2019	2020 WL 5038780	14-Apr-20
Perdue v. Hy-Vee, Inc Filed: 10/2019	455 F.Supp.3d 749, 550 F.Supp.3d 572	20-Apr-20
<i>In re</i> Solara Medical Supplies, LLC Customer Data Security Breach	613 F.Supp.3d 1284	7-May-20
Jantzer v. Elizabethtown Community Hospital Filed: 7/2019	2020 WL 2404764	12-May-20
Culbertson et al. v. Deloitte Consulting LLP (combined with Bozin v. Deloitte Consulting LLP) Filed: 05/2020	2020 WL 4597260	4-Jun-20
Sweet v. BJC Health Systems	2021 WL 2661569	19-Jun-20
Banc of America Merchant Services, LLC v. Arby's Restaurant Group, Inc.	2021 WL 2695474, 2021 WL 2695455	19-Jun-20
Esquer v. StockX, LLC [Case closed] Filed: 09/2020 (five other class actions filed, MDL denied to combine them)	2020 WL 3487821	26-Jun-20
<i>In re</i> Sonic Corp. Customer Data Security Breach Litigation	2021 WL 5916743	1-Jul-20
Young v. Wetzel	260 A.3d 281	2-Jul-20
George D. v. NCS Pearson, Inc. Filed: 2019	2020 WL 3642325	6-Jul-20
Weiss v. Equifax, Inc. Filed: 2020	2020 WL 3840981	8-Jul-20
Tiamson v. Equifax, Inc. Filed: 12/2019 (combined with Nguyen)	2020 WL 3972582	14-Jul-20
Martinez v. NCH Healthcare System, Inc Filed: 05/2020	2020 WL 8679632	14-Jul-20

Case Name	Citation	First Case
Bessemer System Federal Credit Union v. Fiserv Solutions, LLC Filed: 05/2019	472 F.Supp.3d 142	14-Jul-20
Blahous v. Sarrell Regional Dental Center for Public Health, Inc. Filed: 10/2019	2020 WL 4016246	16-Jul-20
Hiscox Insurance Company Inc. v. Warden Grier, LLP Filed: 03/2020	474 F.Supp.3d 1004	23-Jul-20
Kylie S. v. Pearson PLC 09/2019	475 F.Supp.3d 841	28-Jul-20
Smallman v. MGM Resorts International Filed 02/21/2020	2021 WL 326135	31-Jul-20
Patao v. Equifax, Inc Filed: 12/2019 (pro se plaintiff)	2020 WL 5033561	25-Aug-20
Dearing v. Magellan Health Incorporated Filed: 04/2020	2020 WL 7041059	3-Sep-20
Smahaj v. Retrival-Masters Creditors Bureau, Inc. Filed: 2020	131 N.Y.S.3d 817	4-Sep-20
Locke v. Wetzel	2021 WL 1229949	11-Sep-20
<i>In re</i> Capital One Consumer Data Security Breach Litigation Filed: 04/2020	488 F.Supp.3d 374	18-Sep-20
Davis v. Equifax, Inc. (just enforcing a judgment)	2020 WL 6128993	30-Sep-20
Foster v. Health Recovery Services, Inc. (Frechette v. Health Recovery Services, Inc.)(class cert denied)	2020 WL 6440262	7-Oct-20
Griffey v. Magellan Health Incorporated	562 F.Supp.3d 34	8-Oct-20
GreenState Credit Union v. Hy-Vee, Inc.	549 F.Supp.3d 969	11-Oct-20
Hartigan v. Macy's, Inc.	501 F.Supp.3d 1	5-Nov-20
Reidinger v. Zendesk, Inc	2020 WL 6562335, 2022 WL 614235	9-Nov-20
<i>In re</i> Warner Music Group Data Breach	2021 WL 725728	10-Nov-20

Case Name	Citation	First Case
Schmidt v. Experian Information Solutions, Inc.	2022 WL 1417316	13-Nov-20
Stasi v. Inmediata Health Group Corp	2021 WL 5861563	19-Nov-20
Fus v. CafePress, Inc.	2020 WL 7027653	30-Nov-20
<i>In re</i> Hanna Andersson and Salesforce.Com Data Breach Litigation Filed: 02/2020	2020 WL 10054678	29-Dec-20
<i>In re</i> Rutter's Inc. Data Security Breach Litigation	2021 WL 29054, 511 F.Supp.3d 514	5-Jan-21
Abernathy v. Brandywine Urology Consultants, P.A	2021 WL 211144	21-Jan-21
Cohen v. Northeast Radiology, P.C.	2021 WL 293123	28-Jan-21
Flores-Mendez v. Zoosk, Inc.	2022 WL 357500, 2022 WL 2967237	30-Jan-21
Masciotra v. Vertafore, Inc.	2021 WL 1720860	3-Feb-21
Hymes v. Earl Enterprises Holdings, Inc.	2021 WL 1781461	10-Feb-21
Stoll v. Musculoskeletal Institute, Chartered	2020 WL 6784115	18-Feb-21
Clemens v. ExecuPharm, Inc.	2021 WL 735728, 14 F.4th 146	25-Feb-21
Springmeyer v. Marriott International, Inc.	2021 WL 809894	3-Mar-21
Gardiner v. Walmart Inc.	2021 WL 4992539	5-Mar-21
McFarlane v. Altice USA, Inc	524 F.Supp.3d 264	8-Mar-21
Allgood v. Paperlesspay Corporation	2022 WL 846070	11-Mar-21
Darnell v. Wyndham Capital Mortgage, Inc.	2021 WL 1124792	24-Mar-21
Keach v. BST & Co. CPAs, LLP	71 Misc.3d 1204(A)	30-Mar-21
Finesse Express, LLC v. Total Quality Logistics, LLC	2021 WL 1192521	30-Mar-21
Newman v. Total Quality Logistics, LLC	2021 WL 1192669	30-Mar-21
Gaston v. FabFitFun, Inc.	2021 WL 6496734	2-Apr-21
<i>In re</i> Ambry Genetics Data Breach Litigation	567 F.Supp.3d 1130	7-Apr-21

Case Name	Citation	First Case
<i>In re</i> Blackbaud, Inc., Customer Data Breach Litigation	567 F.Supp.3d 667	8-Apr-21
Mullinix v. US Fertility, LLC	2021 WL 4935976	21-Apr-21
Oeste v. Zynga, Inc.	2021 WL 1785139	5-May-21
<i>In re</i> Wawa, Inc. Data Security Litigation	2021 WL 3276148, 2021 WL 2073758, 2022 WL 1173179	6-May-21
Travis v. Assured Imaging LLC	2021 WL 1862446	10-May-21
Atkinson v. Minted, Inc.	2021 WL 2411041	14-May-21
Graham v. Universal Health Service, Inc.	539 F.Supp.3d 481	17-May-21
Peiran Zheng v. Live Auctioneers LLC	2021 WL 2043562	21-May-21
Maldonado v. Solara Medical Supplies, Inc. (details not available through multiple sources)	2021 WL 8323636	2-Jun-21
<i>In re</i> Accellion, Inc., Customer Data Security Breach Litigation	543 F.Supp.3d 1372	7-Jun-21
<i>In re</i> Citrix Data Breach Litigation	2021 WL 2410651	10-Jun-21
Browne v. US Fertility, LLC	2021 WL 2550643	22-Jun-21
Winzig v. Stockpile Investments, Inc.	2021 WL 4812956	2-Jul-21
Cotter v. Checkers Drive-In Restaurant	2021 WL 3775008	7-Jul-21
McCreary v. Filters Fast LLC	2021 WL 3044228	19-Jul-21
Mackey v. Belden, Inc.	2021 WL 3363174	3-Aug-21
<i>In re</i> GE/CBPS Data Breach Litigation	2021 WL 3406374	4-Aug-21
Schmitt v. SN Servicing Corporation	2021 WL 5279822	9-Aug-21
Baldwin v. National Western Life Insurance Company	2021 WL 4206736	15-Sep-21
Purvis v. Aveanna Healthcare, LLC	563 F.Supp.3d 1360	27-Sep-21
Quintero v. Metro Santurce, Inc.	2021 WL 5855752	13-Oct-21
Legg v. Leaders Life Insurance Company	574 F.Supp.3d 985	6-Dec-21

Case Name	Citation	First Case
<i>In re</i> American Medical Collection Agency (AKA Retrival-Masters Creditors Bureau), Inc., Customer Data Security Breach Litigation	2021 WL 5937742	16-Dec-21
Stanberry v. Fox	2021 WL 5999308	20-Dec-21