Chapter 17

Data Breach Litigation

Margaret A. Dale & David A. Munkittrick*

Proskauer Rose LLP

* The authors would like to thank Rucha Desai and Emily Kline for their contributions to this chapter.

§ 17:1 Introduction

While consumer class action litigation following a data breach now seems routine, with lawsuits filed after every report of a major and not-so-major breach, the jurisprudence in the area is actually only about ten years old. And while a data breach can be perpetrated in any number of ways, the legal issues that arise from the theft or loss of data largely fall within the same set of legal paradigms. The focus of this chapter is to survey the development of the law in the area of consumer class action litigation.

§ 17:2 Consumer Plaintiff Theories of Liability

§ 17:2.1 Causes of Action

As can be expected in a developing area like data breach litigation, plaintiffs' liability theories span a range of federal and state statutory and common law claims. Of course, each theory is premised on unauthorized access to personal information and the alleged harm of identity theft or the increased risk of identity theft. There are staple causes of action: negligence, breach of contract, fraud, violation of consumer protection statutes, violation of federal statutes with private rights of action,[1] breach of fiduciary duty, and invasion of privacy, among others. The following subsections review some of the nuances of these theories specific to the data breach context.

[A] Negligence

Almost every data breach case includes a common law claim for negligence. Negligence claims require a standard set of elements: a duty to exercise reasonable care and a failure to exercise that care, which caused actual damage.[2] To establish a duty of care in a data breach case, plaintiffs often point—not always successfully—to alleged promises made by defendants regarding data security or to

---

1. Depending on the context of the data breach and the type of data involved, these can include the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), and the Stored Communications Act (SCA), to name a few. *See supra* chapters 2, 3, and 6.
2. *See, e.g.*, Willingham v. Glob. Payments, Inc., 2013 WL 440702 (N.D. Ga. 2013); Irwin v. RBS Worldpay, Inc., 2010 WL 11570892 (N.D. Ga. Feb. 5, 2010); McLoughlin v. People's United Bank, Inc., 2009 WL 2843269 (D. Conn. 2009); Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc., 2009 WL 799760 (E.D. La. 2009); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009); Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307 (S.D.N.Y. 2008).

industry-specific security protocols.[3] A duty of care can also be established by statute or precedent. For instance, the Gramm-Leach-Bliley Act has been found to impose a duty on financial institutions to protect the security and confidentiality of customers' nonpublic personal information.[4] In Pennsylvania, the state's Supreme Court has found that employers have a common law duty to use reasonable care to safeguard employees' personal information stored on an internet-accessible computer.[5]

[B] Breach of Contract

Breach of contract theories are probably the second most common theories alleged. A contractual relationship in the data breach context can arise from a retail transaction, such as the acceptance of credit or debit card for payment in exchange for goods or services.[6] A company's privacy policy can also be the basis for a breach of contract claim by its customers.[7]

[C] Fraud

Fraud allegations usually involve a claim that a defendant misrepresented the state of its data security or fraudulently concealed a data breach.[8] Such claims are brought under common law fraud theories or at times under state consumer protection laws.[9]

---

3. *See, e.g.*, *Willingham*, 2013 WL 440702, at *18; *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011) (PIN pad security requirements); *see also* chapter 16, *supra* (for more on such security standards).
4. *See* Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483, at *3 (D. Minn. Feb. 7, 2006).
5. Dittman v. UPMC, 196 A.3d 1036 (Pa. 2018).
6. *See* Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 780 (W.D. Mich. 2006); *Michaels Stores*, 830 F. Supp. 2d at 531 (finding sufficient allegations of an implied contract with customers to "take reasonable measures to protect the customers' financial information").
7. *See* Yunker v. Pandora Media, Inc., 2014 WL 988833, at *5 (N.D. Cal. Mar. 10, 2014). Plaintiffs have also couched their contract claims in terms of implied contract. *See* Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *1 (E.D. La. July 14, 2014). An implied contract is formed where the parties' conduct is assumed to have created an enforceable agreement. Order, Irwin v. RBS Worldpay, Inc., 2010 WL 11570892 (N.D. Ga. Feb. 5, 2010).
8. *See* Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307, at *11 (S.D.N.Y. June 25, 2010); *see also infra* section 17:3.1[C] (discussing *Hammond*).
9. *See, e.g.*, *Michaels Stores*, 830 F. Supp. 2d at 529.

§ 17:2.2 Actual Damages

The common law theories of liability, such as negligence, breach of contract, and fraud, all require actual damages.[10] As discussed in more detail below, many plaintiffs fail to adequately plead this element.

§ 17:3 Defense Strategies

Just as plaintiffs' theories of liability continue to evolve in response to the growing volume of reported data breach decisions (still mostly on motions to dismiss), so too do defense strategies. The mainstay defense continues to be Article III standing, challenging whether plaintiffs have adequately alleged an injury in fact, a causal relationship between the alleged conduct and the injury, and a likelihood that a favorable ruling will redress the injury. Decisions on standing in the data breach context now proliferate, with significant distinctions among the circuits. The discussion that follows surveys the current, controlling Supreme Court and circuit court positions, as well as representative district court opinions.

§ 17:3.1 Standing

[A] The Supreme Court on Standing

Depending on the type of data at issue and the type of business the defendant runs, data breach plaintiffs often include statutory causes of actions, from the FCRA to HIPAA. Even where statutes provide for a private right of action, standing is a threshold issue. In 2016, the Supreme Court addressed the question of "whether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm . . . by authorizing a private right of action based on a bare violation of a federal statute."[11] The answer was, as these things often go, "it depends." In so answering, however, the Supreme Court reaffirmed the bedrock requirement of some "concrete injury" in order to satisfy Article III.

Writing for the majority, Justice Alito observed, "We have made it clear time and time again that an injury in fact must be both concrete *and* particularized. . . . A 'concrete' injury must be *'de facto'*; that is,

---

10. *See, e.g.*, Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc., No. 08-1568, 2009 WL 799760, at *1 (E.D. La. Mar. 24, 2009); *Hammond*, 2010 WL 2643307, at *2 (an element of breach of contract is resulting damage).
11. Petition for Writ of Certiorari, Spokeo, Inc. v. Robins, No. 13-1339 (U.S. May 2014), http://sblog.s3.amazonaws.com/wp-content/uploads/2014/05/13-1339-Spokeo-v-Robins-Cert-Petition-for-filing.pdf.

it must actually exist."[12] A plaintiff "could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."[13] While *Spokeo* was not a data breach case, the decision has since taken a prominent role in privacy litigation generally, including data breach litigation.

The claim in *Spokeo* was brought under the FCRA. Robins, the plaintiff, alleged that Spokeo (an online "people search engine") failed to "follow reasonable procedures to assure maximum possible accuracy of" consumer reports and disseminated erroneous information about him.[14] The district court dismissed for failure to plead injury in fact. The Ninth Circuit reversed, concluding that "the violation of a statutory right is usually a sufficient injury in fact to confer standing [and] Robins' alleged violations of his statutory rights were sufficient to satisfy the injury-in-fact requirement of Article III."[15] Vacating that holding, the Supreme Court held it was an "incomplete" injury-in-fact analysis, as it considered only the "particularized" prong and did not determine whether the alleged injury was "concrete," "actually exists[ed]," was real, and not abstract.[16]

The "it depends" result arises from the fact that Congress has "the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before."[17] Still, Congress cannot abrogate the constitutional requirements of Article III. Article III standing requires actual harm to a plaintiff, not merely noncompliance with statutory requirements. As the *Spokeo* Court observed, "a violation of one of the FCRA's procedural requirements may result in no harm. . . . [N]ot all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code."[18] After *Spokeo*, courts are taking a closer look at statutory claims to determine whether they actually caused any concrete injury-in-fact.

Spokeo, however, did not address an alleged risk of future harm, the type of harm often alleged in data breach cases. The Supreme

---

12. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).
13. *Id.* at 1549.
14. *Id.* at 1545.
15. *Id.* at 1546.
16. *Id.* at 1545.
17. *Id.* at 1549 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring)).
18. *Id.* at 1550. On remand, the Ninth Circuit found Robins did have standing, finding the alleged injury was sufficiently concrete: "sufficiently more likely to harm his concrete interests than the Supreme Court's example of an incorrect zip code." Robins v. Spokeo, Inc., 867 F.3d 1108, 1117 (9th Cir. 2017). Spokeo sought review by the Supreme Court again, but the Court declined. 2018 U.S. LEXIS 850 (U.S. Jan. 22, 2018).

Court had addressed that issue in its seminal 2013 *Clapper* decision.[19] In *Clapper*, plaintiffs challenged the constitutionality of 2008 amendments to the Foreign Intelligence Surveillance Act (FISA) that empowered the Foreign Intelligence Surveillance Court to authorize surveillance of persons reasonably believed to be outside the United States.[20] Plaintiffs, U.S. citizens and organizations, alleged that their international communications would likely be acquired under such surveillance in the future.[21] The Supreme Court found that such an allegation of future injury was too speculative because it relied on assumptions that the government would decide to target persons with whom plaintiffs communicate, that the government would invoke FISA to do so, that the government would succeed in intercepting such communications, and that the plaintiffs would be parties to the particular communications intercepted.[22] This did not satisfy the requirement of "certainly impending" harm required for standing.[23]

The *Clapper* plaintiffs also alleged that they suffered present injury in the form of costly and burdensome measures to protect the confidentiality of their international communications.[24] The Supreme Court found this insufficient to confer standing: "[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."[25] Both of these holdings, as to present and future injury, have found direct application in data breach cases.

A third aspect of *Clapper* is relevant in the data breach context. To establish Article III standing, an injury must, in addition to being "concrete, particularized, and actual or imminent," be "fairly traceable to the challenged action."[26] The speculative chain required to reach an actual, imminent injury also meant the challenged conduct in *Clapper* could not be fairly traced to such injury absent speculation.[27]

A second Supreme Court decision has also seen play in the data breach context, though it is not a data breach case either. In *Susan B. Anthony List v. Driehaus*, plaintiffs brought a pre-enforcement challenge to an Ohio statute that prohibited certain false statements

---

19. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).
20. *Id.* at 1150; *see also* chapter 7, *supra* (for further discussion of intelligence gathering under FISA).
21. *Id.* at 1143.
22. *Id.* at 1148.
23. *Id.* at 1143.
24. *Id.*
25. *Id.*
26. *Id.* at 1140–41 (citing Monsanto Co. v. Geertson Seed Farms, 561 U.S. 129 (2010)).
27. *Id.* at 1148–50.

during the course of a political campaign.[28] Again, the issue of future harm was front and center. The plaintiffs alleged that they intended future dissemination of information criticizing votes relating to the Patient Protection and Affordable Care Act.[29] The district court had dismissed the suit on the ground that it did not present a sufficiently concrete injury to meet standing or ripeness requirements, and the Sixth Circuit affirmed. However, the Supreme Court reversed,[30] finding the threat of future enforcement was substantial given the history of past enforcement and that such enforcement proceedings were not rare.[31]

[B] Data Breach Standing in Circuit Courts of Appeals

While the Supreme Court has not had recent occasion to decide a data breach case, many of the circuits have. Soon after *Clapper*, it appeared the decision may have signaled the death knell of private data breach litigation because very few data breach plaintiffs could actually show "certainly impending" injury.[32] However, subsequent decisions in certain circuit courts indicate otherwise, with a circuit split developing.

In July 2015, the first federal appellate court to apply *Clapper* to a data breach case found the plaintiffs had sufficiently alleged injury to confer standing.[33] In 2013, hackers stole customer credit card numbers from a Neiman Marcus database, and several customers brought a class action seeking various forms of relief. The district court

---

28. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334 (2014).
29. *Id.* at 2339.
30. Susan B. Anthony List v. Driehaus, 805 F. Supp. 2d 412 (S.D. Ohio 2011), *aff'd*, 525 F. App'x 415 (6th Cir. 2013), *cert. granted*, 134 S. Ct. 2334, *rev'd and remanded*, 574 F. App'x 597 (6th Cir. 2014).
31. 134 S. Ct. at 2345–46.
32. *See, e.g.*, Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 466 (D.N.J. 2013) (dismissing putative class action for lack of standing where there was no allegation the information was actually read, reviewed, understood, or misused, leading the court to find *Clapper*'s "certainly impending" standard was not met); *In re* Barnes & Noble Pin Pad, 2013 U.S. Dist. LEXIS 125730, at *8 (N.D. Ill. Sept. 3, 2013) (dismissing for lack of standing in the absence of any allegation of the required "certainly impending" injury, notwithstanding an allegation of actual fraudulent charges to one of plaintiff's credit cards because there was no allegation that the plaintiff was not reimbursed or otherwise suffered actual harm as a result).
33. Remijas v. Neiman Marcus Grp. LLC, 794 F.3d 688, 694 (7th Cir. 2015).

dismissed for lack of standing, but the Seventh Circuit reversed.[34] The plaintiffs pointed to six general types of injury:

(1) lost time and money resolving fraudulent charges;

(2) lost time and money protecting themselves from future identity theft;

(3) financial loss of buying items at Neiman Marcus that they would not have purchased if they had known of the store's cybersecurity vulnerabilities;

(4) lost control over the value of their personal information;

(5) increased risk of future fraudulent charges; and

(6) greater susceptibility to identity theft.[35]

The latter two constituted allegations of future harm sufficient to establish standing.

Citing the Northern District of California's decision in *In re Adobe Systems, Inc. Privacy Litigation*, the Seventh Circuit found the plaintiffs had adequately alleged a certainly impending injury.[36] Allegations that the hackers specifically targeted Neiman Marcus and that the plaintiffs' credit card information had actually been stolen left an "objectively reasonable likelihood" that identity theft would occur in the future.[37] The court found the plaintiffs need not wait for the threatened harm to actually occur. The Seventh Circuit affirmed its approach to standing a year later in *Lewert v. P.F. Chang's China Bistro*, finding standing based on the risk of fraudulent charges and identity theft, as well as on fraudulent charges already incurred.[38]

In a 2017 decision, the D.C. Circuit followed the Seventh Circuit's lead, finding plaintiffs had standing in the aftermath of a cyberattack on health insurance companies that involved credit card numbers, social security numbers, sensitive health information, and other personal information. The court reversed dismissal for lack of standing,

---

34. Remijas v. Neiman Marcus Grp. LLC, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014), *rev'd and remanded*, 794 F.3d 688 (7th Cir. 2015).
35. 794 F.3d at 692, 694.
36. *Id.* at 693 (citing *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)).
37. *Id.* (quoting *Clapper*, 133 S. Ct. at 1147).
38. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); *see also* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018) (finding that the plaintiffs had standing because they alleged, *inter alia*, that they had spent time dealing with the consequences of the data theft and, "the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective").

finding persuasive the Seventh Circuit's observation that "[w]hy else would hackers break into a . . . database and steal consumers' private information [if not] to make fraudulent charges or assume those consumers' identities."[39] In finding plaintiffs had plausibly alleged a certainly impending harm, the court noted in particular plaintiffs' description of "'medical identity theft' in which a fraudster impersonates the victim and obtains medical services in her name."[40] This, the court held, "at the very least" created "a plausible allegation that plaintiffs face a substantial risk of identity fraud."[41]

The Ninth Circuit is also largely in line with the Seventh Circuit. In a pre-*Clapper* decision, it found standing in a case where data was stolen but there was no actual identity theft.[42] In *Krottner v. Starbucks*, plaintiff employees were found to have standing where a laptop with employee information was stolen. The threat of future identity theft, the court found, was "credible," "both real and immediate," and "not conjectural or hypothetical."[43] This satisfied Article III.[44]

Not all circuits have reached the same result. Taking the opposite approach of the D.C. Circuit, the Eighth Circuit expressly distinguished the Seventh Circuit. "Although others have ruled that a complaint could plausibly plead that the theft of a plaintiff's personal or financial information creates a substantial risk that they will suffer identity theft sufficient to constitute a threatened injury in fact, we conclude that plaintiffs have not done so here."[45] First, the court noted the type of data alleged to be stolen: credit card information.

---

39. Attias v. Carefirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017) (quoting Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015)); *see also* Attias v. CareFirst, Inc., No. 15-CV-00882 (CRC), 2019 WL 367984 (D.D.C. Jan. 30, 2019) (finding on remand that two of the plaintiffs had alleged actual economic injury sufficient for standing).
40. *Attias*, 865 F.3d at 628.
41. *Id.*
42. Krottner v. Starbucks, 628 F.3d 1139, 1142 (9th Cir. 2010); *see also In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018) (finding that plaintiffs who had not suffered financial losses as the result of a data breach had standing based on the substantial risk of future fraud and identity theft).
43. *Krottner*, 628 F.3d at 1143.
44. Nevertheless, the district court's dismissal under *Iqbal* and *Twombly* was affirmed by the Ninth Circuit due to the plaintiffs' failure to adequately plead "actual loss or damage," a necessary element of the negligence claim, or the existence of an implied contract. Krottner v. Starbucks, 406 F. App'x 129, 131 (9th Cir. 2010).
45. *In re* Supervalu, Inc., 870 F.3d 763, 770 (8th Cir. 2017) (citing Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015)); *see also In re* SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *1 (D. Minn. Mar. 7, 2018) (dismissing on remand for lack of standing).

Without accompanying personally identifying information such as social security numbers, birth dates, or driver's license numbers, "compromised credit or debit card information . . . generally cannot be used alone in opening unauthorized new accounts."[46] In making this finding, the court relied on a U.S. Government Accountability Office report cited in plaintiffs' complaint, which also concluded that "most breaches have not resulted in detected incidents of identity theft" from fraudulent credit or debit card purchases.[47] Based on this, the court found, plaintiffs had not sufficiently alleged a substantial risk of identity theft.[48]

The Third Circuit, in *Reilly v. Ceridian Corp.*, affirmed the district court's ruling that similar allegations of future injury were too speculative to establish standing.[49] In that case, the defendant suffered a security breach in 2009 when an unknown hacker potentially gained access to personal and financial information of approximately 27,000 people. The plaintiffs asserted claims of negligence and breach of contract. The court reasoned that any future injury relied on conjecture that the hacker:

(i) read, copied, and understood the plaintiffs' personal information;

(ii) intended to use the information for future crimes; and

(iii) could use the information to the plaintiffs' detriment.

For the Third Circuit, "unless and until these conjectures come true, [plaintiffs] have not suffered any injury."[50]

---

46. *In re* Supervalu, Inc., 870 F.3d at 770 (citing June 2007 U.S. Government Accountability Office report cited by plaintiffs in their complaint).
47. *Id.* at 771.
48. Highlighting the fact-specific nature of the standing inquiry, even at the pleading stage, the Eighth Circuit had, just nine days before, found plaintiff investor had standing to bring suit against a securities brokerage firm, but only for contract-related claims because the plaintiff alleged "he did not receive the full benefit of his bargain with Scottrade [of] data management and security." Nevertheless, the Eighth Circuit found that the complaint had been properly dismissed for failure to state a claim. Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017).
49. Reilly v. Ceridian Corp., 2011 WL 735512 (D.N.J. Feb. 22, 2011), *aff'd*, 664 F.3d 38 (3d Cir. 2011).
50. *Id.*, 664 F.3d at 46. In a summary, non-precedential opinion, the Second Circuit effectively joined the Third Circuit in holding that allegations of stolen credit card information and attempted but unsuccessful fraudulent purchases failed the "future injury [that is] 'certainly impending' rather than simply speculative" requirement, particularly as the plaintiff had canceled her credit card after the fraudulent attempts. Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017).

Following the Seventh Circuit, however, the Sixth Circuit distinguished *Reilly*, finding future harm to be a concrete injury-in-fact where the data breach was an "intentional theft of [plaintiffs'] data."[51] The Sixth Circuit addressed a case arising from a data breach suffered by an insurance company where none of the plaintiffs had suffered identity theft. The court noted that the breach in *Reilly* was not an "intentional or malicious" invasion.[52]

In a 2017 decision, the Fourth Circuit raised the prospect of a circuit split on the issue of whether alleged nefarious intent behind a data breach suffices to allege standing. In *Beck v. McDonald*,[53] the Fourth Circuit addressed two data breaches at the VA Medical Center—one of a stolen laptop containing a patient's personal information, and the other of four boxes containing personal information. The court noted that "not all threatened injuries constitute an injury-in-fact"[54] and declined to follow the Sixth, Seventh, and Ninth Circuit decisions finding standing in part based on allegations that "the data thief intentionally targeted the personal information compromised in the data breaches."[55] Though the Fourth Circuit indicated it "must assume that the thief targeted the stolen items for the personal information they contained," any risk of harm still required the "attenuated chain of possibilities" rejected in *Clapper* and *Reilly*, as even after the theft, "the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities."[56] Further distancing itself from the Sixth and Seventh Circuits, the Fourth Circuit held

> Contrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals [because] to adopt such a presumption would

---

51. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 390 (6th Cir. 2016).
52. *Id.* at 389.
53. Beck v. McDonald, 848 F.3d 262 (4th Cir.), *cert. denied sub nom.* Beck v. Shulkin, 137 S. Ct. 2307 (2017).
54. *Id.* at 271.
55. *Id.* at 274.
56. *Beck*, 848 F.3d at 275; *see also* Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 2018 WL 2927626 (4th Cir. 2018) (affirming that a "mere compromise of personal information, without more" fails to satisfy the injury-in-fact requirement, but finding that the plaintiffs had sufficiently alleged actual harm because their data had been used to open credit card accounts and plaintiffs had incurred out-of-pocket costs for credit monitoring services and lost the value of their time dealing with the breach).

> surely discourage organizations from offering these services to data-breach victims.[57]

Although the Third Circuit had declined to find standing based on risk of future identity theft in *Reilly*, in 2017, the court, applying *Spokeo*, found standing where two laptop computers containing personal identifying information were stolen from the headquarters of an insurance company.[58] *Spokeo* applied more prominently than *Clapper* in that case because the plaintiffs brought a statutory cause of action under the FCRA, claiming that the defendant "furnished" their information to unauthorized individuals (thieves).[59] The court noted that "unauthorized disclosures of information have long been seen as injurious," citing right of privacy cases, and found "the alleged disclosure of [the plaintiffs'] personal information created a de facto injury."[60] Thus, in the FCRA context at least, disclosure of personal information to unauthorized individuals by reason of a data breach may be enough to confer standing.

In a pre-*Clapper* decision, the Eleventh Circuit, in *Resnick v. AvMed, Inc.*, considered a case that included allegations of actual identity theft as well as future harm.[61] It held the plaintiffs had standing to sue a health insurance company after a company laptop with unencrypted data was stolen and the plaintiffs were subsequently victims of identity theft. In addition to finding the alleged injury (identity theft) was fairly traceable to defendant's conduct, the *Resnick* court reversed the district court's holding that the plaintiffs had not sufficiently pled causation and damages to survive a motion to dismiss. This holding led to a first-of-its-kind settlement of a data breach case, discussed below.[62]

While *Resnick* involved actual identity theft, the First Circuit in *Katz v. Pershing* considered a case that was filed before any data breach.[63] It held that plaintiff's allegations of an increased risk of potential future loss due to the defendant's alleged failure to adhere to reasonable security practices and privacy regulations did not confer standing.[64] The allegations of harm were too speculative, and the

---

57. *Id.* at 276.
58. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625 (3d Cir. 2017).
59. *Id.* at 631.
60. *Id.* at 629.
61. Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012).
62. *See* Curry v. AvMed, Inc., 2014 U.S. Dist. LEXIS 48485 (S.D. Fla. Feb. 28, 2014) (discussed in section 17:4, *infra*).
63. Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012).
64. *Id.* at 78.

plaintiff could not show impending injury.[65] According to the First Circuit, the facts alleged left too many unknown variables, including whether the plaintiff's data would actually be stolen or lost, and even then, whether the data would be misused in a way that would harm the plaintiff. The court recognized, however, that the question of standing would be more difficult if data had actually been stolen, noting the "disarray" in decisions applying an "increased risk of harm" theory to data breach cases absent identity theft.[66]

A circuit decision, of course, does not necessarily lead to uniformity in future district court decisions, and no two data breach cases are exactly alike. Sometimes seemingly subtle factors like the type of data accessed or the method of access will mean the difference between standing and no standing. For example, a network hack of a point-of-sale system containing credit and payment card information may be more likely to be exploited than a stolen laptop with encrypted, relatively more innocuous data such as work history. Accordingly, not all data breach plaintiffs in the Eleventh Circuit, for example, will be found to have standing, even after *Resnick*. Indeed, in a case arising from a hack of MAPCO Express, Inc.'s computer systems, the Northern District of Alabama found *Resnick* left it "not entirely clear . . . whether the allegation of actual identity theft alone or the allegation of actual identity theft plus the allegation of monetary damages prompted the *Resnick* majority to find that the *Resnick* plaintiffs had standing to pursue their identity theft claims."[67] The court went on to dismiss the complaint without prejudice for lack of standing, noting "this is [still] largely unchartered territory."[68]

[C] Standing Decisions in U.S. District Courts

While the D.C., Sixth, Seventh, and Ninth Circuits found allegations of future risk of identity theft sufficient to confer standing, many district courts have found such allegations alone are not sufficient. As the District of Louisiana observed:

> Following *Clapper*, the majority of courts faced with data breach class actions where complaints alleged personal information was accessed but where actual identity theft was not alleged . . . have

---

65. *Id.* at 80.
66. *Id.*
67. Burton v. MAPCO Express, Inc., 47 F. Supp. 3d 1279, 1284 (N.D. Ala. 2014). *But see* Smith v. Triad of Alabama, LLC, 2015 WL 5793318 (M.D. Ala. Sept. 29, 2015) (noting *Burton* is not binding and that "there is no precedent binding on this court stating that for standing purposes, a victim of identity theft *must* allege that he or she suffered economic damages").
68. *Id.*

> dismissed the complaints for lack of Article III standing [because] the mere increased risk of identity theft or identity fraud alone does not constitute a cognizable injury unless the harm alleged is certainly impending.[69]

Where allegations of potential injury are "contingent upon . . . information being obtained and then used by an unauthorized person," courts usually have not found standing.[70] In *Key v. DSW, Inc.*, for instance, the plaintiff alleged that "unauthorized persons obtained access to and acquired the information of approximately 96,000 customers."[71] She alleged she had "been subjected to a substantial increased risk of identity theft or other related financial crimes,"[72] but the court dismissed for lack of standing finding the plaintiff had not "alleged evidence that a third party intend[ed] to make unauthorized use of her financial information or of her identity."[73]

Similarly, the U.S. District Court for the District of Minnesota declined to find standing in a case brought on behalf of a purported class of SuperValu customers, despite an allegation that one of the sixteen named plaintiffs suffered identity theft following two data breaches of the grocery store chain. The court found the allegations of future risk of harm were too speculative and not imminent, noting in particular that over a year had passed since the breach.[74] Applying the traceability prong of standing analysis, the *SuperValu* court found that an allegation of a single fraudulent charge in the year and a half following a data breach was not traceable to the breach.[75] The court distinguished its prior decision in *In re Target Corp. Customer Data Security Breach Litigation*, where customers had alleged more "widespread" and "substantial data misuse which plausibly suggested that the hackers succeeded in stealing the data and were willing and able to use it for future theft or fraud."[76]

Plaintiffs also often argue that they will incur actual harm in the form of purchasing credit monitoring services. This argument is often rejected as overlooking "the fact that [the] expenditure of time

---

69. Green v. ebay Inc., 2015 U.S. Dist. LEXIS 58047, at *1–2, *10 (E.D. La. May 4, 2015) (following "the majority of district courts" in holding "the increased risk of future identity theft or identity fraud posed by a data security breach" does not confer Article III standing) (citations omitted).
70. Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006).
71. *Id.* at 686.
72. *Id.*
73. *Id.* at 690.
74. *In re* SuperValu, Inc., 2016 WL 81792 (D. Minn. Jan. 7, 2016).
75. *Id.* at *5.
76. *Id.* at *6 (distinguishing *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014)).

and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized."[77]

Even where plaintiffs allege actual fraudulent credit card charges as a result of the data breach, courts have dismissed for lack of standing where the plaintiffs were not held financially responsible for paying the fraudulent charges. In *Peters v. St. Joseph Services Corp.*, hackers infiltrated a healthcare provider's network and accessed personal information of patients and employees, including bank account information.[78] There was an attempted purchase on plaintiff's credit card, but it was declined by the plaintiff when she received a fraud alert. As such, there was no injury to confer standing, and any future risk was too speculative and attenuated. Each of plaintiff's alleged harms, the court pointed out, began with the word "if."[79]

Similarly, in *Amburgy v. Express Scripts, Inc.*, the Eastern District of Missouri found that the string of "if's" linking the data breach to the alleged injuries was fatal to standing.[80] The plaintiffs in *Amburgy* filed suit after unauthorized persons accessed the defendant's database that held personal information including contact information and Social Security numbers. It was unclear what data, if any, the hackers obtained. The alleged harm—identity theft—could only come about "'if' this personal information was compromised, and 'if' such information was obtained by an unauthorized third party, and 'if' his identity was stolen as a result, and 'if' the use of his stolen identity caused him harm."[81] Finding this risk of future harm too attenuated from the data breach to confer standing, the court dismissed the case.

Still, standing decisions are mixed, even within a district. The Southern District of New York, for example, has come out on both sides. In *Hammond v. Bank of New York Mellon Corp.*, the court granted summary judgment for the defendant, dismissing all claims and finding no Article III standing where the plaintiffs alleged only an increased risk of identity theft resulting from a loss of data.[82]

---

77. Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006); *see also* Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8 (D.D.C. 2007). *But see Neiman Marcus*, 794 F.3d at 694 (noting "[m]itigation expenses do not qualify as actual injuries where the harm is not imminent," while finding it "telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information," and that that cost "easily qualifies as a concrete injury").
78. Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847 (S.D. Tex. 2015).
79. *Id.* at 854.
80. Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009).
81. *Id.* at 1053.
82. Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307, at *6–9 (S.D.N.Y. June 25, 2010).

Hammond arose out of the loss of computer backup tapes containing personal information. A few of the named plaintiffs in *Hammond* experienced unauthorized payment card transactions, but they admitted they could not connect the unauthorized transactions to the data loss other than by a coincidence of timing. Thus, the alleged injuries stemming from the data loss remained "speculative" and "hypothetical," and the action was dismissed for lack of standing.[83] By contrast, the court two years earlier had held in *Caudle v. Towers, Perrin, Forster & Crosby, Inc.* that increased risk of future harm was sufficient to confer standing, analogizing to toxic tort cases.[84] More recently, district courts within New York have found standing even where the plaintiffs had not alleged any misuse of their personal information because of the substantial threat of future harm from exposure of, among other things, their dates of birth and Social Security numbers.[85]

Distinguishing factors among the cases are not always clear, and range from legal interpretation of standing doctrine to the type of information stolen or hacked. At least one court, for instance, has interpreted the Supreme Court's *Driehaus* decision as relegating *Clapper*'s more rigorous "certainly impending" standard to national security cases.[86] The court in *Green v. eBay* distinguished decisions finding standing as involving stolen credit or debit card numbers, while the plaintiff in *Green* did not allege that any financial information was stolen.[87]

---

83. *Id.* at *8.
84. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281 (S.D.N.Y. 2008).
85. Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d 333 (W.D.N.Y. 2018) (finding that plaintiffs who had not alleged any misuse of their personal information had standing based on the substantial threat of future harm for exposure of their dates of birth and Social Security numbers); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739 (S.D.N.Y. 2017) (finding that risk of future harm was sufficient for standing where plaintiff's names, addresses, dates of birth, SSNs, and bank account information had been exposed).
86. *See* Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *5 (E.D. La. July 14, 2014) (concluding that the Supreme Court's decision in *Driehaus* indicates *Clapper*'s imminence standard is a rigorous standing analysis to be applied only in cases that involve national security or constitutional issues); *see also supra* section 17:3.1[A] (discussing *Clapper* and *Driehaus*).
87. Green v. eBay, 2015 WL 2066531, n.34 (E.D. La. May 4, 2015) (distinguishing *In re* Adobe Sys., Inc. Privacy Litig., 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014), and *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014)).

§ 17:3.2 Failure to State a Claim upon Which Relief Can Be Granted (Rule 12(b)(6))

Even where a court finds standing, however, some data breach cases are dismissed under Rule 12(b)(6) of the Federal Rules of Civil Procedure for failure to state a claim. Plaintiffs, even with standing, must still adequately plead damages and causation, necessary elements in most common law causes of action arising from data breaches. As courts have recognized, these are often difficult elements to plead, because even in cases of actual identity theft, there is little information to causally connect the data breach to the specific instance of identity theft.[88]

The Seventh Circuit in *Pisciotta*, for example, found standing with little discussion and focused instead on the question of whether the plaintiffs' alleged injuries were compensable under Indiana law. The court answered no and affirmed dismissal of the case.[89] The U.S. District Court for the Northern District of Illinois similarly dismissed a case under Rule 12(b)(6) where the plaintiff did not plead economic or out-of-pocket damages caused by a data breach, a required element of the plaintiff's breach of contract causes of actions.[90] Similarly, the Ninth Circuit allowed *Krottner v. Starbucks* to proceed after finding standing, but later affirmed dismissal for failure to adequately plead damages.[91] The *Krottner* plaintiffs failed to establish a cognizable injury for their negligence claim because the alleged injuries stemmed from the threat of future harm. The applicable state law was clear that "the mere danger of future harm, unaccompanied by present damages, will not support a negligence action."[92]

---

88. *See Burton*, 47 F. Supp. 3d at 1280 ("Under the pleading standard that the United States Supreme Court enunciated in *Ashcroft v. Iqbal*, [556 U.S. 662 (2009),] it is difficult for consumers like Mr. Burton to assert a viable cause of action stemming from a data breach because in the early stages of an action, it is challenging for a consumer to plead facts that connect the dots between the data breach and an actual injury so as to establish Article III standing."); *but see* Razuki v. Caliber Home Loans, Inc., No. 17CV1718-LAB (WVG), 2018 WL 2761818 (S.D. Cal. June 8, 2018) (holding that the plaintiff had sufficiently alleged causation at the pleading stage, since all reasonable inferences are drawn in the plaintiff's favor and he had alleged that he gave defendant private data, a breach occurred, and someone tried to open credit card accounts in his name).
89. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).
90. *In re* Barnes & Noble Pin Pad Litig., 2016 WL 5720370 (N.D. Ill. Oct. 3, 2016).
91. *Krottner*, 406 F. App'x at 131.
92. *Id.*

One of the largest data breach cases emerged a much smaller case after defendants' motion to dismiss.[93] The plaintiffs had brought fifty-one causes of action, including claims sounding in negligence, breach of contract, violation of consumer protection statutes, violation of the California Database Breach Act, and violation of the Fair Credit Reporting Act. The defendants first argued that *Clapper* tightened the standing analysis, which had been governed by the Ninth Circuit's pre-*Clapper* decision in *Krottner v. Starbucks*.[94] But the district court disagreed, finding the *Krottner* analysis in line with *Clapper*. It held that, by alleging personal information was collected and then wrongfully disclosed as a result of the data breach, plaintiffs had standing.[95]

Despite finding standing, most but not all of plaintiffs' claims were dismissed for failure to state a claim. For example, negligence theories were dismissed for failure to plead harm and causation with sufficient particularity, and under the economic loss doctrine. Still, the court upheld consumer fraud claims based on misrepresentations and omissions regarding reasonable network security and industry-standard encryption, as well as claims under the California Database Breach Act, which sets forth standards and requirements for disclosing a data breach and includes a private right of action.

The Third Circuit took a similar approach in *Longenecker-Wells v. Benecard Services, Inc.*[96] *Longenecker* arose from a data breach of the plaintiffs' employer, after which the plaintiffs suffered financial harm when unknown third parties filed fraudulent tax returns and the IRS issued refunds to those third parties but not to plaintiffs. While this was enough to confer standing, the Third Circuit affirmed dismissal of plaintiffs' negligence and breach-of-implied-contract claims under Rule 12(b)(6). The plaintiffs' negligence claims failed because Pennsylvania law precluded negligence claims that result "solely in economic damages unaccompanied by physical injury or property damage," and the breach-of-implied-contract claim failed because the plaintiffs failed to adequately plead the existence of an implied contract.[97]

In *McLoughlin v. People's United Bank, Inc.*, the applicable state law required an "ascertainable loss," and the court found an increased

---

93. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014).
94. Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
95. *Sony*, 996 F. Supp. 2d at 961–62.
96. Longenecker-Wells v. Benecard Servs., Inc., 658 F. App'x 659 (3d Cir. 2016).
97. *Id.*; *but see Dittman*, 196 A.3d at 1048–56 (holding that Pennsylvania's economic loss doctrine permits recovery for purely pecuniary damages in a negligence claim premised on an employer's breach of their duty to use reasonable care to safeguard employees' personal information).

risk of identity theft did not constitute an ascertainable loss absent actual misuse of the stolen data.[98] The court, citing New York law, noted that "an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy."[99] And in *Grigsby v. Valve Corp.*, the Western District of Washington dismissed a putative class action brought after a hacking incident in which a third party breached the defendant's internet security system and accessed users' personal account information.[100] The court found that "when personal information is compromised due to a security breach, there is no cognizable harm absent actual fraud or identity theft."[101]

The *Grigsby* court addressed the plaintiffs' allegations of present harm under the *Iqbal/Twombly* pleading standards, finding insufficient general allegations of interruption to various services and subscriptions, "loss of data," an "inability to access various gaming networks," and a loss of "the monies paid to Defendant for products and services which do not conform to the express warranties made by Defendant."[102] Without specific allegations regarding which services were interrupted, which networks were inaccessible, what data was lost, and how any money was lost, the complaint constituted "naked assertions" that did not give the defendant fair notice of the basis for the claims. It "did not raise entitlement to relief above the speculative level."[103]

In short, for the few cases that survive a Rule 12(b)(1) motion contesting standing, even fewer survive a Rule 12(b)(6) motion.

§ 17:3.3 Surviving Other Motions

For the cases that survive a motion to dismiss for lack of standing and failure to state a claim, procedurally the next important decision points include motions for summary judgment and for class certification. And while settlement may occur before or after the motions to dismiss are decided, for defendants that continue to defend themselves, a loss on summary judgment or on class certification generally leads to settlement.

---

98. McLoughlin v. People's United Bank, Inc., 2009 U.S. Dist. LEXIS 78065, at *19–20 (D. Conn. 2009).
99. *Id.* at *22.
100. Grigsby v. Valve Corp., 2012 U.S. Dist. LEXIS 179096, at *3 (W.D. Wash. 2012).
101. *Id.* at *6.
102. *Id.* at *12.
103. *Id.* at *12–13.

[A] Motions for Summary Judgment

Take, for example, the case of *Forbes v. Wells Fargo Bank, N.A.*[104] The dispute in *Forbes* arose from the allegedly negligent protection of personal data. Defendant Wells Fargo Bank and subsidiaries of Wells Fargo hired a service provider, Regulus Integrated Solutions, to print monthly statements for certain home equity mortgage and student loan customers. On October 3, 2004, computers were stolen from Regulus that contained unencrypted customer information including names, addresses, Social Security numbers, and account numbers. Plaintiffs Kristine Forbes and Morgan Koop were among the customers whose information was on one of the stolen computers. After discovery, the court rejected plaintiffs' claim that their money spent on credit-monitoring services established damages, and granted defendant's motion for summary judgment, dismissing the case.[105]

[B] Motions for Class Certification

Another hurdle for consumer class action plaintiffs is class certification. Rule 23 of the Federal Rules of Civil Procedure sets forth the necessary elements for a case to proceed as a class action. The element that is often at issue in data breach cases is the predominance requirement. To certify and maintain a class action, Rule 23 requires that "the court find[ ] that the questions of law or fact common to class members predominate over any questions affecting only individual members."[106]

With respect to the predominance requirement, the case of *In re Hannaford Brothers* is instructive. There the court distinguished between individualized damages issues that would not defeat class certification and individualized causation issues that would.[107] In *Hannaford*, a grocery store was hacked, and the credit card information of the store's customers was stolen. Following a dismissal of earlier claims for lack of standing, the plaintiffs eventually sought to certify a class of people that spent money mitigating the breach by paying fees to replace their credit cards and purchasing credit and identity theft monitoring. The court found that individual issues would predominate when it came to what caused the alleged damages. It recognized that customers may have replaced their cards or purchased insurance for reasons unrelated to the breach. The court also acknowledged that credit card fraud is pervasive and may have

---

104. Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006).
105. *Id.* at 1021.
106. FED. R. CIV. P. 23(b)(3).
107. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 293 F.R.D. 21, 26 (D. Me. 2013).

happened for reasons unrelated to the breach. The court denied certification because the plaintiffs had not presented an expert opinion to overcome the predominance issues related to causation and damages. The *Hannaford* court's analysis may impact settlement values because plaintiffs may need to present expert testimony to support their novel causation and damages theories before a class can be certified.

The requirement that the class representatives "fairly and adequately protect the interests of the class" has also posed a hurdle in data breach litigations. Fed. R. Civ. P. 23(a)(4). In 2018, the Northern District of Illinois denied a motion to approve class settlement and decertified the proposed class, finding that the class representatives could not satisfy the adequacy requirement.[108] In that case, malware had compromised customer credit card payment information at several Neiman Marcus locations. The class comprised three groups: (1) customers who had used payment cards at affected locations during the period when the malware was installed; (2) customers who had used payment cards during the period when the malware was in use, but at stores not affected by the malware; and (3) customers who had used payment cards at times when no malware was present in any store.[109] The problem, the court found, was the different remedies to the three groups. The second and third groups did not have an available monetary remedy, while the first group did. This created a conflict among the class representatives, the court reasoned. The members who could recover damages were incentivized to maximize the monetary recovery, whereas the other members would prefer stronger injunctive relief (the court described the non-monetary relief in the settlement as "lackluster").[110] The court held that the named plaintiffs could not adequately represent the class due to this "fundamental conflict" between the class members.[111]

While most data breach actions settle before a motion to certify the class is decided, *Smith v. Triad of Alabama LLC* became the first consumer data breach case to certify a class.[112] In that case, a hospital employee stole patient records and filed over 120 fraudulent tax returns. Several affected patients sued the hospital for violations of the Fair Credit Reporting Act, negligence, negligence per se and breach of contract. Defendants argued that the class was not ascertainable

---

108. Remijas v. Neiman Marcus Grp., LLC, 341 F. Supp. 3d 823 (N.D. Ill. 2018).
109. *Id.*
110. *Id.*
111. *Id.*
112. Smith v. Triad of Ala., LLC, No. 1:14-CV-324-WKW, 2017 WL 1044692, at *1 (M.D. Ala. Mar. 17, 2017), *on reconsideration in part*, No. 1:14-CV-324-WKW, 2017 WL 3816722 (M.D. Ala. Aug. 31, 2017).

because it included members who had alleged that their identities were "merely stolen," not actually misused, and therefore did not have Article III standing.[113] The court rejected this argument, noting that the Eleventh Circuit has not required a showing of actual misuse to prove standing. Defendants also argued that the typicality requirement was not met because some plaintiffs had signed the hospital's notice of privacy practices, which created an express contract, while some plaintiffs had not, and thus had only an implied contractual relationship with the hospital. The court held that this did not defeat typicality, and resolved the issue by dividing the class into two subclasses, one for the express contact claims and one for the implied contract claims. While damages and causation were individualized issues, the court found that they did not defeat predominance because the common issues of contract formation and breach, and the hospital's duty of care and breach of that duty, were "crucial" to the case and "answering [those] questions one way or another [would] effectively decide the parties' dispute."[114] As the first consumer class action to achieve certification, *Smith v. Triad* provides illuminating guidance to plaintiffs and defendants navigating motions for class certification.

§ 17:4 Non-Consumer Plaintiffs

While consumer class actions make up the bulk of data breach litigation, data breaches often spawn a number of other types of private lawsuits as well, from insurance litigation to shareholder derivative suits. This section touches on several such areas of litigation: shareholder derivative suits, enforcement actions brought by state attorneys general, securities suits, and claims brought by financial institutions.[115]

§ 17:4.1 Shareholder Derivative Suits

In an October 2015 speech discussing cases in which "shareholders have sued boards of directors for failing to guard against cyberattacks, alleging breaches of fiduciary duties and oversight failures," SEC Commissioner Aguilar emphasized "the increasing importance of a board's oversight role in risk management"[116] Indeed, shareholder derivative suits have followed high-profile data breaches suffered by Target, Wyndham Hotels, and Home Depot in 2014 and 2015.

---

113. *Id.* at *5.
114. *Id.* at *12.
115. *See* chapter 16, *supra* (discussing insurance issues).
116. Luis A. Aguilar, Comm'r, U.S. Sec. & Exch. Comm'n, The Important Work of Boards of Directors, Remarks Before the 12th Annual Boardroom Summit and Peer Exchange (Oct. 14, 2015).

Plaintiffs in all three cases alleged instances where the company officers and directors failed to properly provide for and oversee an information security program, and to promptly and accurately disclose the breach, claiming damage to company reputation and finances. Each suit, however, was defeated on a motion to dismiss.[117]

§ 17:4.2 Attorney General Suits

State attorneys general have become more active in litigating data breach cases (as opposed to just opening investigations). For example, the Massachusetts Attorney General brought suit against Equifax, Inc. after the 2017 data breach that involved the personal information, including social security numbers, of 148 million people. The Massachusetts AG sued Equifax for violations of the state's Data Breach Notification Law, Data Security Regulations, and Consumer Protection Act.[118] Denying Equifax's motion to dismiss for failure to state a claim, the Massachusetts Superior Court found that Equifax's alleged failure to maintain an adequate security program and take reasonable steps to keep its data secure could plausibly have violated state data security regulations, and that Equifax's alleged misrepresentations concerning the security of their data systems could constitute unfair or deceptive acts. The court further held that the Attorney General did not have to prove that any consumers were actually harmed because "unlike a private litigant . . . [the Attorney General] is only required to prove that unfair or deceptive acts or practice took place in trade or commerce" in order to claim statutory penalties.[119]

§ 17:4.3 Securities Suits

Data breaches have also spawned securities fraud lawsuits, where plaintiff shareholders bring claims related to the loss of value of their shares in the aftermath of a data breach. In a suit brought against Equifax, Inc., the plaintiffs claimed that Equifax made false or misleading statements and omissions about the sensitive personal

---

117. *In re* Target Corp. S'holder Derivative Litig., No. 0:14-cv-00203 (D. Minn. Jan. 21, 2014) (dismissed after report of Target's Special Litigation Committee determined it was not in Target's interest to pursue derivative actions against directors and officers); Palkon v. Holmes, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014) (granting motion to dismiss based on business judgment rule); *In re* Home Depot, Inc. S'holder Derivative Litig., 2016 U.S. Dist. LEXIS 164841 (N.D. Ga. Jan. 20, 2016) (granting motion to dismiss for failure to allege facts excusing plaintiffs' failure to demand that the board take the desired action, a prerequisite to suit).

118. Commonwealth v. Equifax, Inc., No. 1784CV03009BLS2, 2018 WL 3013918, at *1 (Mass. Super. Apr. 3, 2018).

119. *Id.*

information in their custody, the vulnerability of their internal systems to cyber-attack, and their compliance with data protection laws and cybersecurity best practices, which artificially inflated the value of Equifax's securities.[120] The court partially denied the defendants' motion to dismiss, finding the plaintiffs had adequately alleged false statements as well as the requisite scienter against the CEO, but not as to the director defendants.[121]

Equifax is not unique in facing data breach securities lawsuits. Several prominent companies faced such suits, including Marriot, Alphabet Inc. (Google's parent company), Chegg (an educational services company), and Huazhu Group (a Chinese hotel group). In each, shareholders alleged that the company (and/or its executives) made false and misleading disclosures regarding its security measures. And in the Chegg and Huazhu complaints, plaintiffs also alleged that the company's stock price dropped as a result of the breach, and that the allegedly false and misleading disclosures led to artificially inflated stock prices.[122]

§ 17:4.4 Claims Brought by Financial Institutions

Financial institutions have found more success in joining the data breach fray. While consumers allege increased risk of identity theft and time and expense spent on identity protection, financial institutions commonly file suit seeking to recoup costs associated with replacing cards and reimbursing customers for fraudulent purchases.[123] One of the first such cases was brought on a negligence theory and was addressed by Fifth Circuit in 2013.[124] As in consumer class actions involving negligence theories, the defendant argued for the application of the economic loss doctrine, which precludes recovery in tort where there is no actual personal injury or harm to property. After the district court dismissed on that basis, however, the Fifth Circuit reversed because, "In the absence of a tort remedy, the [plaintiffs] would be left with no remedy for [defendant's] alleged

120. *In re* Equifax Inc. Sec. Litig., No. 17-CV-3463-TWT (N.D. Ga. Jan. 28, 2019).
121. *Id.*
122. McGrath v. Marriot Int'l, Inc., No. 18-06845 (E.D.N.Y. filed Dec. 1, 2018); Wicks v. Alphabet Inc., No. 4:18-cv-06245 (N.D. Cal. filed Oct. 11, 2018); Bao v. Page, No. 3:19-cv-00314 (N.D. Cal. filed Jan. 18, 2019); Shah v. Chegg, Inc., No. 18-05956 (N.D. Cal. filed Sept. 27, 2018).
123. *E.g.*, Bellwether Cmty. Credit Union v. Chipotle Mexican Grill, Inc., No. 17-CV-1102-WJM-STV, 2018 WL 5279468 (D. Colo. Oct. 24, 2018).
124. Lone Star Nat'l Bank v. Heartland Payment Sys., 729 F.3d 421 (5th Cir. 2013).

negligence, defying notions of fairness, common sense and morality."[125] After remand, the case settled.

Jurisprudence of financial institution data breach cases is even younger than that of consumer class actions. Writing in September 2016, the Southern District of Illinois noted that suits by financial institutions were still "relatively new territory in the data breach context."[126] The plaintiff banks in that case brought "an impressive 13 different theories of relief," from fraud to breach of fiduciary duty, negligence, and breach of contract, after the defendant Schnuck Markets suffered a data breach of "potentially 2.4 million [payment] cards."[127] The court dismissed the claims under Rule 12(b)(6), however, because the plaintiffs failed to plead injury and other elements of their claims with the requisite particularity.[128] The Seventh Circuit affirmed the dismissal, holding that the remedies available to the plaintiffs were limited to contract law because the relationships between the parties involved in the compromised transactions were defined by contract, at least some of which included data security provisions.[129]

As noted in the following section, however, a number of financial institution suits have survived motions to dismiss and reached significant settlements.[130]

§ 17:5 Noteworthy Settlements

There have been numerous settlements of data breach class actions, arising at different points in the proceedings. The following is a survey of some of those settlements.

Heartland. In *In re Heartland Payment System, Inc. Customer Data Security Breach Litigation*,[131] hackers stole payment card information

---

125. *Id.* at 427.
126. Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 2016 U.S. Dist. LEXIS 133482, at *8–9 (S.D. Ill. Sept. 28, 2016).
127. *Id.* at *6.
128. *Id.* at *34, *52 (finding, for instance, that the plaintiffs "failed to make out a plausible claim for negligence misrepresentation because they have not identified any concrete misrepresentations, they have not alleged facts sufficient to suggest there was a duty between the parties, and they have not specifically addressed the economic loss doctrine").
129. Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803 (7th Cir. 2018).
130. *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014) (granting in part and denying in part motion to dismiss); *In re* Home Depot, Inc. Customer Data Sec. Breach Litig., 2016 U.S. Dist. LEXIS 65111 (N.D. Ga. May 17, 2016) (granting in part and denying in motion to dismiss).
131. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 851 F. Supp. 2d 1040 (S.D. Tex. 2012).

for 100 million consumers from a payment processing company. The Judicial Panel on Multidistrict Litigation transferred the resulting class action lawsuits to the Southern District of Texas for consolidated pretrial proceedings. Heartland settled the case and agreed to make up to $2.4 million available to customers.

In re Ashley Madison. In July 2015, Ashley Madison, a dating website to help individuals cheat on their spouses, announced that its website had been breached, exposing personal details of over 37 million users. The breach led to blackmail and even suicides. Consumers filed multiple class actions, and two years later, in July 2017, Ashley Madison agreed to pay up to $3,500 to users with valid claims, up to a total of $11.2 million, one third of which would cover legal fees.[132]

AvMed. The 2014 settlement in *Curry v. AvMed, Inc.*[133] was considered cutting-edge because it was the first time that plaintiffs who did not suffer identify theft were allowed to claim funds. The case stemmed from a 2009 theft from health insurer AvMed of laptop computers that contained the personal information of 1.2 million customers. And while the district court had dismissed the claims in July 2011 based on a lack of injury, the Eleventh Circuit reversed and reinstated the case on the basis that the plaintiffs had made an explicit connection between the stolen materials and the subsequent opening of fake bank accounts.[134] The case settled for $3 million and included payment to customers of $10 for each year of insurance they purchased (up to a cap of $30).

Adobe. In 2013, hackers attacked Adobe's servers and spent several months inside the network without being detected, removing customer data (including payment card information) and Adobe source code in the process. Plaintiffs sued, arguing that Adobe failed to implement reasonable, industry-standard security procedures (such as employing intrusion detection systems and properly segmenting source code and customer payment card data) that would have prevented or minimized the impact of the data breach.[135] The breach affected 38 million Adobe users. The case settled after the court granted in part and denied in part Adobe's motion to dismiss.[136] The plaintiffs filed a partially redacted motion in the U.S. District Court for the Northern District of California seeking voluntary dismissal

---

132. *In re* Ashley Madison Customer Data Sec. Breach Litig., No. 15-md-02669 (E.D. Mo. July 14, 2017).
133. Curry v. AvMed, Inc., 2014 U.S. Dist. LEXIS 48485 (S.D. Fla. Feb. 28, 2014).
134. Resnick v. Avmed, Inc., 693 F.3d 1317, 1327 (11th Cir. 2012).
135. Consolidated Class Action Complaint, *In re* Adobe Sys., Inc. Privacy Litig., 2014 WL 1841156 (N.D. Cal. Apr. 4, 2014).
136. *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

of the class claims pursuant to the no-fault settlement. Adobe agreed to pay $5,000 per named plaintiff and $1.2 million in legal fees and expenses, and agreed to additional security enhancements. The settlement is noteworthy because there was no evidence of actual damages or identity theft.

Anthem. In February 2015, Anthem, Inc. announced it had suffered a massive data breach affecting tens of millions of its health insurance customers. Multiple class actions followed and were consolidated in the Northern District of California.[137] The parties ultimately reached a $115 million settlement, including up to $38 million in attorneys' fees.[138] The settlement also set aside $15 million to reimburse out-of-pocket costs, and provided two years of credit monitoring for class members.

LinkedIn. In June 2012, LinkedIn announced that hackers had stolen about 6.5 million users' passwords and published them on a Russian website. Multiple class actions were consolidated in the Northern District of California. Initially, the case was dismissed because of the failure to allege cognizable harm. Subsequently, the plaintiffs filed an amended complaint claiming that LinkedIn had misled its customers about its data protection policies. After the court partially granted and partially denied LinkedIn's motion to dismiss the second amended complaint,[139] the case settled for $1.25 million. The approximately 800,000 class members were able to receive up to $50 each.

Nationwide Mutual Insurance Co. Thirty-three states reached a $5.5 million settlement with Nationwide Mutual Insurance Company and its subsidiary, Allied Property & Casual Insurance Company, over an October 2012 data breach affecting personal identifying information of 1.27 million people. As part of the settlement, Nationwide is required to update its security practices, including hiring an individual to be responsible "for maintaining the process by which Nationwide/Allied's security policies as to software and application security updates and security patch management are regularly reviewed and by which revisions are made."[140]

---

137. *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 968 (N.D. Cal. 2016); *In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299 (N.D. Cal. 2018) (approving the settlement).
138. *In re* Anthem Inc. Data Breach Litig., No. 5:15-md-02617 (N.D. Cal. June 23, 2017).
139. *In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1095 (N.D. Cal. 2013).
140. Assurance of Voluntary Compliance, *In re* Nationwide Mut. Ins. Co. & Allied Prop. & Cas. Ins. Co. (Aug. 3, 2017), https://ag.ny.gov/sites/default/files/nationwide-aod.pdf.

Target. In December 2013, Target announced that third-party intruders had stolen credit card, debit card, and contact information for 110 million of its customers. Class representatives filed multiple actions alleging common law claims and violations of state laws based on Target's allegedly inadequate data security and alleged delay in notifying Target customers of the breach. The cases were consolidated in the District of Minnesota, and a settlement was achieved in 2015 after the district court's decision, which granted in part and denied in part Target's motion to dismiss.[141] Target agreed to pay $10 million to settle the claims of class members, and the maximum recovery per customer was capped at $10,000.[142] Target also agreed to pay attorney fees and expenses of up to $6.75 million.[143]

After an appeal of the consumer settlement, however, the Eighth Circuit in February 2017 remanded for reconsideration of whether the consumer plaintiffs adequately represent the class, noting that the district court had not applied a sufficiently "rigorous analysis" as was required in certifying a class.[144] In a separate case arising from the Target data breach, a consolidated class action brought by financial institutions reached settlement of $39 million.[145] The class representatives in that case received $20,000, and the court awarded $17.7 million in attorney fees. Separately, Target agreed to pay $18.5 million to resolve an investigation by forty-seven states and the District of Columbia.[146]

---

141. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014).

142. The court granted final approval of the settlement on November 15, 2015, but an appeal of that order was filed by objectors. On January 27, 2016, the Eighth Circuit dismissed the objection, and the settlement is now final.

143. Relatedly, Target settled for $39.4 million the class action lawsuits brought against it by financial institutions in the payment card industry for costs they incurred to replace credit cards of affected Target customers, as well as the costs of the fraudulent charges. That settlement came about after the court denied Target's motion to dismiss, finding the financial institutions had adequately pleaded "a special relationship" with Target. Order, *In re* Target (Fin. Insts. Case), MDL 14-2522 (J.P.M.L. Dec. 2, 2014). Earlier in 2015, Target agreed to pay Visa card issuers as much as $67 million over the breach.

144. *In re* Target Corp. Customer Data Sec. Breach Litig., 847 F.3d 608 (8th Cir. 2017).

145. *In re* Target Corp. Customer Data Sec. Breach Litig., 2016 U.S. Dist. LEXIS 63125 (D. Minn. 2016).

146. In the Matter of Investigation by Eric T. Schneiderman, Attorney Gen. of the State of N.Y., of Target Corp., Assurance No. 17-094.

Home Depot. Between April and September 2014, Home Depot suffered one of the largest retail data breaches at the time.[147] A consumer class brought claims for violations of state consumer laws, state data breach statutes, negligence, breach of implied contract, unjust enrichment, and for declaratory judgment. Home Depot filed a motion to dismiss, but before the motion was argued, the parties reached settlement. Home Depot agreed to pay for eighteen months of credit monitoring service and establish a $13 million settlement fund. The agreement capped individual recovery at $10,000 "because many class members in data breach cases suffer very small losses."[148] In March 2017, Home Depot settled a separate class action brought by several financial institutions for $25 million. Entities with valid claims could receive up to $2 for every compromised credit or debit card, in addition of up to 60% of uncompensated losses from the breach.[149] Class attorneys were awarded $15.3 million in fees.[150] One month later, Home Depot investors settled their shareholder derivative suit, which alleged board members breached their duty of loyalty to the company by not preventing or remedying the breach. The settlement required Home Depot to institute a series of reforms, and pay up to $1.125 million in attorneys' fees.[151]

Staples. In September 2015, CVS announced that hackers had attacked servers hosted by PNI Digital Media Inc., an online photo center manager acquired by Staples in 2014. In May 2017, a settlement was reached with the plaintiff class, providing customers up to $250 to reimburse bank fees, long-distance calls, and other expenses related to the breach, as well as $10,000 for "extraordinary expenses" and $650,000 to cover attorneys' fees and settlement costs.[152]

Wendy's. In early 2016, Wendy's began investigating a potential data breach and found malware on some of its systems, which had been installed through the use of compromised third-party credentials and affected the point of sale systems at over 1,000 of their locations. Consumers filed a class action for breach of implied contract, negligence, and violations of state business and consumer protection laws.

---

147. *In re* Home Depot, Inc., Customer Data Sec. Litig., 2016 WL 2897520 (N.D. Ga. May 8, 2016).
148. *In re* Home Depot, Inc., Customer Data Sec. Litig., No. 1:14-md-02583-TWT, Dkt. No. 260 (N.D. Ga. Aug. 23, 2016).
149. *In re* The Home Depot Inc., Customer Data Sec. Breach Litig., No. 1:14-md-02583 (N.D. Ga. Mar. 9, 2017).
150. *Id.*
151. *In re* The Home Depot Inc. S'holder Derivative Litig., No. 1:15-cv-2999 (N.D. Ga. Apr. 28, 2017).
152. T.A.N. v. PNI Digital Media Inc., No. 2:16-00132 (S.D. Ga. May 25, 2017).

The parties agreed to a settlement totaling $3.4 million.[153] Affected individuals could collect reimbursement for documented expenses up to $5,000 for a variety of costs associated with mitigating identity theft or fraud and preventative costs, including late fees, overdraft fees, and unauthorized charges. Class members could also collect $15 per hour for time spent resolving issues related to the data breach, up to a total of five hours.

That data breach also led to a suit by financial institutions against Wendy's to recover the reimbursements they made to customers for fraudulent purchases made on the credit and debit cards compromised in the breach.[154] The financial institutions brought claims for negligence, negligence per se, and violations of the Ohio Deceptive Trade Practices Act, alleging that numerous deficiencies in Wendy's security systems had caused those systems to be susceptible to a data breach. They further accused Wendy's of taking a "lackadaisical" approach to data security and ignoring the "well-publicized and ever-growing threat of cyber-attacks targeting payment card data."[155] Wendy's agreed to pay $50 million and adopt reasonable safeguards to manage data security risks to settle the case.

Yahoo. In early 2019, the Northern District of California denied a motion for preliminary approval of a class action settlement.[156] The court said the settlement inadequately disclosed the release of certain claims and improperly released those claims, and that Yahoo's refusal to disclose the total amount to be paid out to those affected rendered it insufficient. The court also criticized the settlement for not disclosing the costs of credit monitoring services, class notice, or settlement administration, and not disclosing the total size of the settlement fund and settlement class. The court disapproved of the nonmonetary relief, which did not require security enhancements. The court also chastised the plaintiff's lawyers for insufficiently investigating the data breach, allowing unauthorized lawyers to work on the case, and requesting inordinate legal fees (up to $35 million).

---

153. Torres v. Wendy's Int'l, LLC, No. 6:16-cv-210-PGB-DCI (M.D. Fla. Feb. 25, 2019).

154. First Choice Fed. Credit Union v. Wendy's Co., No. 216CV00506NBFMPK, 2019 WL 948400 (W.D. Pa. Feb. 26, 2019) (granting preliminary approval).

155. Consol. Amended Class Action Complaint, First Choice Credit Union v. Wendy's Co., No. 2:16-cv-00506-NBF-MPK, 2016 WL 11480103 (W.D. Pa. July 22, 2016).

156. *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK (N.D. Cal. Jan. 1, 2019).