DEFENDING SECURITY BREACH CLASS ACTION LITIGATION

Excerpted from Chapter 27 (Cybersecurity: Information, Network and Data Security) of
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

PRIVACY + SECURITY FORUM
GEORGE WASHINGTON UNIVERSITY
WASHINGTON, D.C.
OCTOBER 14-16, 2019

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:	Los Angeles:
1900 University Avenue, 5th Fl.	1840 Century Park East, Ste. 1900
East Palo Alto, CA 914303	Los Angeles, CA 90067
Direct Dial: (650) 289-7881	Direct Dial: (310) 586-6575
Direct Fax: (650) 462-7881	Direct Fax: (310) 586-0575

Ballon@gtlaw.com
<www.ianballon.net>
LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition* (Thomson West 2018 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, https://store.legal.thomsonreuters.com/E-Commerce--Internet-Law-Treatise; (888) 728-7677
www.ianballon.net

GT GreenbergTraurig

Ian C. Ballon

Shareholder
Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal Circuits
U.S. Supreme Court
JD, LLM, CIPP/US

Ballon@gtlaw.com
LinkedIn, Twitter, Facebook: IanBallon

Silicon Valley
1900 University Avenue
5th Floor
East Palo Alto, CA 94303
T 650.289.7881
F 650.462.7881

Los Angeles
1840 Century Park East
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Ian Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice and represents Internet, technology, mobile and other companies in intellectual property and internet- and mobile-related litigation, including the defense of data privacy, security breach, and TCPA class action suits. He is also the author of the leading treatise on Internet law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 5-volume set published by West (www.IanBallon.net). In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). He also serves as Executive Director of Stanford University Law School's Center for E-Commerce, which hosts the annual Best Practices Conference where lawyers, scholars and judges are regularly featured and interact. A list of recent cases may be found at http://www.gtlaw.com/Ian-C-Ballon-experience.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2019, 2018, 2016 and 2013 editions of Best Lawyers in America. In both 2018 and 2019 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder*'s 2017 Litigation Departments of the Year Awards. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award for significant contributions to the development of intellectual property law (http://ipsection.calbar.ca.gov/IntellectualPropertyLaw/IPVanguardAwards.aspx). He is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also has been recognized by *The Daily Journal* as one of the Top 75 IP litigators in California in every year that the list has been published, from 2009 through 2019, and has been listed as a Northern California Super Lawyer every year from 2004 through 2018 and as one of the Top 100 lawyers in California. Mr. Ballon also holds the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

27.07 Cybersecurity and Data Breach Litigation

In General

Litigation arising out of a security breach may be brought by or against a business that experienced the loss. A company may choose to pursue civil or criminal remedies against the person or persons responsible for the breach,[1] which in civil actions may require satellite litigation to compel the disclosure of the identity of an anonymous or

---

[Section 27.07]

[1]The tradeoff between civil and criminal remedies for the theft of information and other Internet crimes is analyzed in chapter 43. Crimes and related penalties are analyzed in chapter 44. Remedies for phishing and identity theft are analyzed in chapter 46.

pseudonymous thief.[2] A company that experienced a data loss also may be sued by its customers or other third parties allegedly impacted by the breach, including in putative class action suits. Litigation sometimes arises in tandem with or following a regulatory enforcement action by the Federal Trade Commission or following notice of a breach sent to state Attorneys General or other officials, as required by state law.[3]

Litigation initiated *by* companies that were targeted for a security attack may be brought against employees and contractors or corporate spies and hackers, depending on whether the source of the loss was internal to the company or external, based on trade secret misappropriation (if confidential trade secrets were taken),[4] copyright law[5] or various claims relating to screen scraping, data and database protection[6] (if material taken is copied), the Computer Fraud and Abuse Act[7] or common law trespass[8] (for an unauthorized intrusion), the Electronic Communications Privacy Act[9] (for unauthorized interception of material in transit (such as through the use of key loggers or sniffers) or material in storage) or an array of state law causes of action, including unfair competition and claims for relief under those state

---

[2]*See infra* §§ 37.02 (compelling the disclosure of the identity of anonymous and pseudonymous tortfeasors), 50.06 (service provider obligations in response to civil subpoenas).

[3]*See infra* §§ 27.08 (analyzing state security breach notification laws), 27.09 (reprinting state laws).

[4]*See supra* chapter 10 (misappropriation of trade secrets).

[5]*See supra* chapter 4 (digital copyright law). A security claim may be preempted by the Copyright Act where it amounts to claim based on copying. *See, e.g., AF Holdings, LLC v. Doe,* 5:12-CV-02048-EJD, 2012 WL 4747170, at *2-3 (N.D. Cal. Oct. 3, 2012) (holding that plaintiff's negligence claim based on the theory that Botson had a duty to secure his Internet connection to protect against unlawful acts of third parties was preempted by the Copyright Act because it amounted to little more than the allegation that Botson's actions (or inaction) played a role in the unlawful reproduction and distribution of plaintiff's video in violation of the Copyright Act); *see generally supra* § 4.18 (analyzing copyright preemption).

[6]*See supra* chapter 5 (database protection).

[7]18 U.S.C.A. § 1030; *see generally infra* § 44.08.

[8]*See supra* § 5.05[1] (analyzing computer trespass cases).

[9]18 U.S.C.A. §§ 2510 to 2521 (Title I), 2701 to 2711 (Title II); *see generally infra* §§ 44.06, 44.07.

laws that afford a statutory remedy for a security breach.[10]

Security breaches may give rise to shareholder suits, including suits for securities fraud.[11] Security breach litigation also may arise between companies over responsibility for a breach. The largest number of cases, however, are suits by affected consumers against companies, which typically are brought as putative class action suits.

When companies are sued by consumers or their business customers over a security breach, the most common theories of recovery are breach of contract, breach of implied contract, breach of fiduciary duty, public disclosure of private facts, and negligence, depending on the facts of a given case. Security breach suits brought by consumers against companies that have experienced a breach therefore frequently are framed in terms of common law and state statutory remedies. Those few federal statutes that impose express data security obligations on persons and entities—The Children's Online Privacy Protection Act[12] (which regulates information collected from children under age 13), The Gramm-Leach-Bliley Act (which imposes security obligations on financial institutions[13]) and the Health Insurance Portability and Accountability Act (HIPAA)[14] (which regulates personal health information)—typically do not authorize a private cause of action (although the same underlying conduct that violates obligations under these laws potentially could be actionable under other theories of recovery). Claims also sometimes are asserted under federal computer crime statutes, such as the Stored Communications Act,[15] but those statutes usually aren't well-suited to data breach cases.[16] Claims arising out of security breaches also have been brought under the Fair

---

[10]*See infra* § 27.08[10][C].

[11]*See, e.g., In re The Home Depot, Inc. Shareholder Derivative Litigation,* 223 F. Supp. 3d 1317 (N.D. Ga. 2016) (dismissing complaint against former officers of the corporation, alleging breach of the duty of loyalty, waste of corporate assets, and violation of the Securities and Exchange Act arising out of retail payment card data systems, where demand, pursuant to Federal Rule 23.1, was neither made nor excused).

[12]15 U.S.C.A. §§ 6501 to 6506; *supra* §§ 26.13[2], 27.04[2].

[13]15 U.S.C.A. §§ 6801 to 6809, 6821 to 6827; *supra* § 27.04[3].

[14]42 U.S.C.A. §§ 1320d *et seq.*; *supra* § 27.04[4].

[15]18 U.S.C.A. §§ 2701 to 2711; *see generally supra* § 26.15 (putative privacy class action suits brought under the Stored Communications Act); *infra* §§ 44.07 (analyzing the statute in general), 50.06[4] (subpoenas).

[16]*See, e.g.*, *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699 (N.D. Ill.

Credit Reporting Act,[17] but that statute imposes obligations on consumer reporting agencies, users of consumer reports, and furnishers of information to consumer reporting agencies,[18] and therefore does not provide a general remedy in the case of security breaches if the defendant is not a member of one of those three groups.[19]

2012) (dismissing without prejudice plaintiff's claim under the Stored Communications Act in a putative class action suit brought against a company that stored personal health information, where the plaintiff alleged that the company failed to implement adequate safeguards to protect plaintiff's information when a computer hard drive containing the information was stolen, but could not show that the disclosure was made *knowingly,* as required by sections 2702(a)(1) and 2702(a)(2)); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 523–24 (N.D. Ill. 2011) (dismissing plaintiffs' Stored Communications Act claim in a putative security breach class action suit resulting from a hacker skimming credit card information and PIN numbers from PIN pads in defendant's stores; holding that Michaels Stores was neither an ECS provider nor an RCS provider and therefore not subject to the SCA).

The court's ruling in *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699 (N.D. Ill. 2012) underscores why most security breach cases brought by customers against businesses that experienced security incidents are ill suited to Stored Communications Act claims. In *Worix,* the plaintiff had alleged that MedAssets deliberately failed to take commercially reasonable steps to safeguard sensitive patient data by failing to encrypt or password-protect it. The court, however, explained that "[t]he first of these allegations is beside the point, and the latter is insufficient." Judge Kennelly of the Northern District of Illinois emphasized that "[t]he SCA requires proof that the defendant 'knowingly *divulge[d]*' covered information, not merely that the defendant knowingly failed to protect the data." *Id.* at 703 (emphasis in original), *citing* 18 U.S.C.A. §§ 2702(a)(1), 2702(a)(2). In so holding, the court explained that "knowing conduct includes willful blindness, but not recklessness or negligence." *Id.* at 702.

[17]15 U.S.C.A. §§ 1681 *et seq.*

[18]*Chipka v. Bank of America*, 355 F. App'x 380, 382 (11th Cir. 2009).

[19]*See, e.g.*, *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016) (reversing the lower court's holding that plaintiffs' allegation that the defendant in a security breach case violated the FCRA's statement of purpose in 15 U.S.C.A. § 1681(b) (which plaintiff alleged was actionable under sections 1681n(a) and 1681o) was insufficient to confer statutory standing because it failed to allege a specific violation, without expressing any view of the merits of plaintiffs' claim); *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *3–4 (N.D. Ill. Jan. 21, 2015) (dismissing plaintiff's FCRA claim arising out of a security breach where the plaintiff could not allege that the defendant, an insurance company, was a credit reporting agency, and could not plausibly allege a violation of section 1681e, which requires that every consumer reporting agency maintain reasonable procedures designed to limit the risk of furnishing consumer reports to third parties, because "defendants

Class action lawyers increasingly look to state data security statutes to argue that a breach may have reflected a defendant's failure to adhere to reasonable security or data disposal/ minimization obligations.[20] Where a company fails to provide notice to consumers, it also potentially could be sued for statutory remedies in those states that afford a private cause of action to enforce rights under state security breach notification laws.[21] Public companies that experience data breaches also may be subject to securities fraud class action suits.[22]

A company's obligation to comply with security breach notification laws often results in publicity that leads to litigation, including class action litigation, as well as regulatory scrutiny (which alternatively may lead to litigation).[23]

Higher stakes security breach litigation typically is brought by business customers of a company that has experienced a breach over which party bears the risk of loss.

---

cannot be held liable under the FCRA for improperly furnishing information where that information was stolen by third parties."); *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1286–87 (N.D. Ala. 2014) (dismissing a FCRA claim arising out of a security breach where the defendant was not a consumer reporting agency); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 881–82 (N.D. Ill. 2014) (dismissing a FCRA claim where the defendant in a security breach case was not a "consumer reporting agency," which is defined as an entity engaged in the practice of assembling or evaluating consumer credit information for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing reports, 15 U.S.C.A. § 1681a(f), and could not allege that Trustwave's "purpose" was to furnish the information to data thieves); *In re Sony Gaming Networks & Customer Data Security Breach Litig.*, 996 F. Supp. 2d 942, 1010–12 (S.D. Cal. 2014) (dismissing plaintiffs' Fair Credit Reporting Act claim because Sony was not a consumer reporting agency); *Willingham v. Global Payments, Inc.*, No. 1:12–CV–01157–RWS, 2013 WL 440702, at *13 (N.D. Ga. Feb. 5, 2013) (holding that because "the data was stolen, not furnished . . . [and] Defendant did not transmit or furnish data to the hackers, [Defendant] . . . did not violate [the FCRA]"); *Holmes v. Countrywide Fin. Corp.*, No. 5:08–CV–00295–R, 2012 WL 2873892, at *16 (W.D. Ky. July 12, 2012) (finding that the plaintiff did not adequately allege that defendant furnished financial information to a third-party who had engineered "an elaborate and sophisticated theft").

[20]State data security statutes are addressed generally in section 27.04[6] and in greater detail in other sections cross referenced there.

[21]*See generally infra* § 27.08[10][C].

[22]*See supra* § 27.04[5][B] (S.E.C. guidelines).

[23]*See infra* § 27.08[1] (addressing state security breach laws and cross-referencing cites to notice obligations under federal law).

By contrast, consumers often are insulated from the financial consequences of a security breach.

In cases involving credit card theft, for example, credit card companies sometimes cancel accounts before consumers could be impacted (or refund the maximum $50 charge that a customer could incur as a result of credit card fraud under federal law).[24] While potential plaintiffs may be apprehensive of potential future harm that could result from identity theft, that apprehension may not translate to present injury or damage sufficient to establish Article III standing or state a claim (or, where it is, it may not be directly traceable to a particular breach, or a particular company's responsibility for the breach, as opposed to other factors).

When a breach occurs, and an actual financial loss can be established, a plaintiff may be able to assert claims for breach of contract (including potentially breach of a Terms of Service agreement or privacy policy),[25] breach of fiduciary duty, negligence or similar claims, depending on the facts of a given case.[26] These common law claims rarely afford either statutory damages or attorneys' fees, however, so plaintiffs

---

[24]*See* 15 U.S.C.A. §§ 1643, 1693g; 12 C.F.R. § 205.6(b) (limiting liability for unauthorized charges to $50). A consumer's liability will be capped at $50 only where the consumer reported the loss within two business days of learning about it. Otherwise, the loss may be capped at $500. Where a loss is not reported within sixty days of the time a financial institution transmitted a statement on which the unauthorized loss was shown, the consumer will bear the full loss. *See* 12 C.F.R. § 205.6(b); *see infra* § 31.04[3].

To evaluate whether risk of loss rules for a given transaction are determined by Regulation Z or Regulation E, *see* 12 C.F.R. §§ 205.6(d), 226.12(g).

[25]A privacy policy may also provide a strong defense to these claims.

In one case, a court held that a class could not be certified based on an alleged breach of the defendant's privacy policy for allegedly failing to maintain adequate security, due to lack of commonality, where the issues of incorporation of the Privacy Policy by reference in the defendant's insurance contracts with putative class members and damages raised mixed factual and legal issues under the laws of multiple states. *See Dolmage v. Combined Insurance Company of America*, 2017 WL 1754772, at *5-8 (N.D. Ill. May 3, 2013) ("Given the multiple state laws that would be applied in this case, the Court easily concludes that certification of a nationwide class would be improper. The need to determine the enforceability of the Privacy Pledge under a plethora of state laws weighs strongly against a finding of commonality.").

[26]*See, e.g., In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763 (8th Cir. 2017) (holding that one of 16 plaintiffs who alleged that he suffered a fraudulent charge on his credit card after mak-

who have not incurred any financial loss may have weak claims, if they are viable at all, because damage or injury frequently is an element of an affirmative claim, in addition to a requirement for standing. Security breaches have become so common today that the typical plaintiff has had his or her information exposed—perhaps even multiple times—but has not been the victim of identity theft and has not incurred a financial loss. As a consequence, in many consumer security breach cases where there has been no financial loss, maintaining a claim presents a real obstacle.

A plaintiff in federal court must establish injury to even maintain suit.[27] While there typically is not the same stand-

---

ing a purchase at one of defendants' stores had standing to sue for negligence, breach of implied contract, violations of state consumer protection and data breach notification statutes and unjust enrichment, while the other 15 plaintiffs who merely alleged a threat of future injury did not); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (holding that victims of identity theft had standing to sue for negligence, negligence *per se,* breach of fiduciary duty, breach of contract, breach of implied contract, breach of the duty of good faith and fair dealing and unjust enrichment/restitution, in a suit arising out of the disclosure of sensitive information (including protected health information, Social Security numbers, names, addresses and phone numbers) when two laptops containing unencrypted data were stolen, where plaintiffs had both been victims of identity theft following the breach); *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008) (finding standing to bring a constitutional right to privacy claim where plaintiff's information was posted on a municipal website and then taken by an identity thief, causing her actual financial loss fairly traceable to the defendant's conduct), *cert. denied,* 555 U.S. 1126 (2009).

[27]The Constitution limits the judicial power of the federal courts to actual cases and controversies. U.S. Const. art. III, § 2, cl. 1. A case or controversy exists only when the party asserting federal jurisdiction can show "such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends." *Baker v. Carr*, 369 U.S. 186, 204 (1962). Absent Article III standing, there is no "case or controversy" and a federal court lacks subject matter jurisdiction over the suit. *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 101 (1998); *see also Whitmore v. Arkansas*, 495 U.S. 149, 154–55 (1990) ("Article III . . . gives the federal courts jurisdiction over only 'cases and controversies.' ").

For common law claims, the only standing requirement is that imposed by Article III of the Constitution. "When a plaintiff alleges injury to rights conferred by a statute, two separate standing-related inquiries pertain: whether the plaintiff has Article III standing (constitutional standing) and whether the statute gives that plaintiff authority to sue (statutory standing)." *Katz v. Pershing, LLC*, 672 F.3d 64, 75 (1st Cir. 2012), *citing Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 89, 92 (1998). Article III standing presents a question of justiciability; if it

ing requirement to sue in state court, class action lawyers often prefer to be in federal court to seek certification of

---

is lacking, a federal court has no subject matter jurisdiction over the claim. *Id.* By contrast, statutory standing goes to the merits of the claim. *See Bond v. United States*, 564 U.S. 211, 218-19 (2011).

To establish Article III standing a plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.,* 528 U.S. 167, 180-81 (2000).

To establish injury in fact, a plaintiff must show that he or she has suffered " 'an invasion of a legally protected interest' that is [(a)] 'concrete and particularized' and [(b)] 'actual or imminent, not conjectural or hypothetical.' " *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992); *see also Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013) ("[t]o establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.' "), *quoting Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149-50 (2010).

In the absence of actual harm, the Court made clear in *Spokeo* that intangible harm may satisfy the "injury in fact" prong of the test for standing but "both history and the judgment of Congress play important roles." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016). As discussed later in this section, standing may be shown based on intangible harm where "an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* For cases involving alleged statutory violations, "Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.' " *Id., quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 578 (1992). This second consideration—the judgment of Congress—would not be applicable to common law or even state statutory remedies. It could only serve as a basis for standing in a case involving a federal question claim. One district court held that a state legislature could create rights sufficient to confer Article III standing "[i]n the absence of governing U.S. Supreme Court precedent . . . ," *Matera v. Google, Inc.,* Case No. 15-CV-04062-LHK, 2016 WL 5339806, at *14 (N.D. Cal. Sept. 23, 2016) (denying defendant's motion to dismiss plaintiff's CIPA claim), but this analysis is plainly wrong given that Justice Alito expressly identified the role of *Congress,* not state legislatures, in elevating claims. Moreover, state legislatures have no legal authority to confer jurisdiction over state claims on federal courts. *See, e.g., Hollingsworth v. Perry,* 133 S. Ct. 2652, 2667 (2013) ("[S]tanding in federal court is a question of federal law, not state law. And no matter its reasons, the fact that a State thinks a private party should have standing to seek relief for a generalized grievance cannot override our settled law to the contrary."); *Fero v. Excellus Health Plan, Inc.,* 236 F. Supp. 3d 735 (W.D.N.Y. 2017) (citing *Spokeo* and *Hollingsworth* in finding no standing to sue under various state statutes).

potentially larger national class actions. Even if plaintiffs have not been injured and have no recoverable damages, the potential cost to defending a class action and potential adverse publicity[28] encourage some defendants to settle—

Spokeo established that standing may not be based solely on the violation of a federal statute in the absence of injury in fact. It also clarified when intangible harm may be sufficient to establish injury in fact, while also making clear that bare procedural violations of a statute will be insufficient.

Although some suits involve allegations of intangible harm, injury in fact in a security breach case alternatively may be based on the threat of future harm, such as identity theft or other financial consequences potentially flowing from a security breach. The case most directly relevant to future harm is *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), in which the Court made clear that allegations of "possible future injury" are not sufficient. *Id.* at 409. To justify standing based on future harm, the threatened injury must be "certainly impending" to constitute injury in fact. *Id.* at 410-14. In *Clapper,* the Supreme Court held that U.S.-based attorneys, human rights, labor, legal and media organizations did not have standing to challenge section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.A. § 1881a, based on their allegation that their communications with individuals outside the United States who were likely to be the targets of surveillance under section 702 made it likely that their communications would be intercepted. The Court characterized their fear as "highly speculative" given that the respondents did not allege that any of their communications had actually been intercepted, or even that the U.S. Government sought to target them directly. 568 U.S. at 410. As discussed later in this section, there is currently a circuit split over whether and to what extent a victim of a security breach who is not also a victim of identity theft may have standing to sue based on the threat of future harm, as discussed later in this section.

In rare instances, a suit may be brought where emotional injuries will suffice to establish standing. *See, e.g.*, *Rowe v. UniCare Life and Health Ins. Co.*, No. 09 C 2286, 2010 WL 86391, at *6 (N.D. Ill. Jan. 5, 2010) (denying defendant's motion to dismiss common law negligence, invasion of privacy and breach of implied contract claims where the plaintiff had alleged that he suffered emotional distress, which, if proven, would constitute a present injury resulting from his insurance company's disclosure of insurance identification numbers, Social Security numbers, medical and pharmacy information, medical information about their dependents, and other protected health information; holding that a plaintiff whose personal data had been compromised "may collect damages based on the increased risk of future harm he incurred, but only if he can show that he suffered from some present injury beyond the mere exposure of his information to the public."). Usually, however, the economic loss doctrine bars recovery of damages for potential emotional injuries arising from fear and apprehension of potential identity theft, as discussed later in this section.

[28]Potential concerns about adverse publicity have become less significant as virtually every company and every consumer in America has been

and the larger the class, the greater the value of a potential settlement in the eyes of some plaintiffs' counsel.

Where standing can be established in federal court (or for cases brought in state court, where Article III standing is not an issue), many potential claims still require a showing of injury to survive a motion to dismiss. Even where claims can be maintained, consumer class action suits may raise complicated issues associated with proving causation—especially where a given consumer has had his or her information compromised more than one time[29] or where a company incurred a loss despite taking industry standard precautions to prevent a breach. Finally, even where causation and liability can be established, if there has been no harm, damages may be merely speculative. Plaintiffs' counsel therefore try to focus on claims that afford statutory damages and attorneys' fees and usually prefer to settle cases if they can. Indeed, as of September 2018, no security breach class action suit has ever gone to trial. When cases do settle, the amount of the settlement is usually discounted to account for challenges the plaintiff may face in establishing standing, stating a claim, certifying a class, and getting past summary judgment (with the amount impacted by other recent settlements).

Standing

A threshold question in most security breach putative class action suits filed in federal court is standing. Standing must be established based on the named plaintiffs that actually filed suit, not unnamed putative class members.[30]

---

the victim of a security breach (if not multiple breaches).

[29]For example, the Target and Neiman Marcus security breaches in 2013 both involved the same attack. If a customer used the same credit card at both stores in the same month and then was a victim of identity theft, proving causation could be challenging.

[30]*See, e.g.*, *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976) ("That a suit may be a class action . . . adds nothing to the question of standing, for even named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.' "; quoting *Warth v. Seldin*, 422 U.S. 490, 502 (1975)); *see also O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) ("if none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class."); *Payton v. County of Kane*, 308 F.3d 673, 682 (7th Cir. 2002)

Although plaintiffs' counsel may advance an array of creative theories, in most data breach cases where the plaintiffs have not been the victims of identity theft or otherwise lost money as a result of the breach, their argument for standing typically amounts to apprehension about the possibility of future identity theft. To establish standing based on the threat of future injury, a plaintiff must demonstrate that (a) a threatened injury is "certainly impending" or (b) there is a "substantial risk" that the harm will occur.[31]

Among federal appellate courts, there presently is a circuit split over the issue of what level of harm is sufficient to establish Article III standing in a security breach case. The Seventh,[32] Ninth,[33] and D.C. Circuits,[34] as well as the Sixth

---

("Standing cannot be acquired through the back door of a class action." (internal quotation omitted)); *see also Easter v. American West Financial*, 381 F.3d 948, 962 (9th Cir. 2004) (holding that a court must first evaluate the standing of named plaintiffs before determining whether a class may be certified).

[31]*Susan B. Anthony List v. Driehaus,* 134 S. Ct. 2334, 2341 (2014); *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409-10, 414 n.5 (2013); *In re SuperValu, Inc., Customer Data Security Breach Litig*., 870 F.3d 763, 769 & n.3 (8th Cir. 2017) (explaining that "[t]he Supreme Court has at least twice indicated that both the 'certainly impending' and 'substantial risk' standards are applicable in future injury cases, albeit without resolving whether they are distinct, and we are obligated to follow this precedent."); *Attias v. Carefirst, Inc*., 865 F.3d 620, 626 (D.C. Cir. 2017) (explaining the two alternative grounds on which standing may be based under *Clapper* in a case where the harm alleged is the risk of future injury), *cert. denied*, 138 S. Ct. 981 (2018); *Beck v. McDonald*, 848 F.3d 262, 272, 275 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

[32]*See Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692, 694-95 (7th Cir. 2015) (holding that plaintiffs had standing to sue in a data breach case where their credit card numbers had been compromised, even though they had not been victims of identity theft, where Neiman Marcus's offer of credit monitoring was construed to underscore the severity of the risk and "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); *Lewert v. P.F. Chang's China Bistro Inc.,* 819 F.3d 963, 967-68 (7th Cir. 2016) (applying *Remigas* in finding standing where defendants issued an initial press release advising that debit cards used at all of their restaurants had been compromised, even though this assertion was subsequently corrected to reflect that plaintiffs' information had not been compromised, and where they recommended that customers check their credit cards, based on the present harm caused by plaintiffs having to cancel their cards); *see also Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 827-30 (7th Cir. 2018) (holding that plaintiffs had stated a claim for damages because they had standing to assert California and Illinois state law claims against a merchant for a security breach arising out of

compromised PIN pads used to verify credit card information, where one plaintiff was injured because (1) her bank took three days to restore funds someone else had used to make a fraudulent purchase, (2) she had to spend time sorting things out with the police and her bank. and (3) she could not make purchases using her compromised account for three days; and the other plaintiff alleged that (1) her bank contacted her about a potentially fraudulent charge on her credit card statement and deactivated her card for several days, and (2) the security breach at Barnes & Noble "was a decisive factor" when she renewed a credit-monitoring service for $16.99 per month).

[33]*See In re Zappos.com, Inc.*, 888 F.3d 1020, 1023-30 (9th Cir. 2018) (holding that plaintiffs, whose information had been stolen by a hacker but who had not been victims of identity theft or financial fraud, nevertheless had Article III standing to maintain suit in federal court, relying on the fact that other parties had alleged financial harm from the same security breach, which the court found evidenced the risk to these plaintiffs, who did not allege similar harm but alleged the threat of future harm, and because, after the breach, Zappos provided routine post-breach precautionary advice about changing passwords, which the panel considered to be an acknowledgement by Zappos that the information taken gave the hackers the means to commit financial fraud or identity theft).

The Ninth Circuit in *Zappos* relied on an older opinion that predated the Supreme Court's decision in *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409-10, 414 n.5 (2013), which the panel in *Zappos*, like district courts before it, had interpreted to not be inconsistent with *Clapper. See Krottner v. Starbucks Corp*., 628 F.3d 1139, 1142–43 (9th Cir. 2010) (holding that employees had standing to sue based on their increased risk of future identity theft where a company laptop containing the unencrypted names, addresses, and social security numbers of 97,000 Starbucks employees had been stolen); *In re Yahoo! Inc. Customer Data Security Breach Litig.,* No. 16-MD-02752-LHK, 2017 WL 3727318, at *11-17 (N.D. Cal. Aug. 30, 2017) (holding that plaintiffs had Article III standing, in an opinion in which the court ultimately dismissed a number of plaintiffs' causes of action for failure to state a claim); *Corona v. Sony Pictures Entertainment, Inc.,* No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *2-3 (C.D. Cal. June 15, 2015) (holding that plaintiffs had Article III standing, although ultimately dismissing plaintiff's negligence claim based on an alleged duty to timely provide notice and dismissing with prejudice plaintiffs' claim under the California Records Act, Cal. Civil Code §§ 1798.80 *et seq.*, because plaintiffs did not qualify as "customers" under that statute); *In re Adobe Systems, Inc. Privacy Litig*., 66 F. Supp. 3d 1197, 1211-14 (N.D. Cal. 2014). (following *Krottner,* finding that "*Clapper* did not change the law governing Article III standing," and accordingly holding that plaintiffs had standing to assert claims for declaratory relief and under Cal. Civil Code § 1798.81.5 for Adobe's alleged failure to maintain reasonable security for their data and for unfair competition for failing to warn about allegedly inadequate security in connection with a security breach that exposed the user names, passwords, credit and debit card numbers, expiration dates, and email addresses of 38 million customers);

Circuit[35] in a non-precedential opinion, and district courts elsewhere,[36] apply a very liberal pleading standard in evaluating assertions of standing based on future harm, which makes it easier for plaintiffs to establish standing in data breach cases in those circuits based merely on the potential future risk of financial harm or identity theft.

By contrast, the Fourth[37] and Eighth[38] Circuits, as well as

---

In re Sony Gaming Networks & Customer Data Security Breach Litig., 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014) (construing *Krottner* as consistent with *Clapper* in finding standing in a security breach case).

Even in the Ninth Circuit, the threat of future harm will be found too tenuous to support standing where there has not yet even been a breach. *See, e.g., Cahen v. Toyota Motor Corp.,* 717 F. App'x 720 (9th Cir. 2017) (affirming the lower court's ruling finding no standing to assert claims that car manufacturers equipped their vehicles with software that was susceptible to being hacked by third parties).

[34]*See Attias v. Carefirst, Inc.,* 865 F.3d 620 (D.C. Cir. 2017) (following the Seventh Circuit's decision in *Remijas v. Neiman Marcus Group, LLC*, in holding that plaintiffs, whose information had been exposed but who were not victims of identity theft, had plausibly alleged a heightened risk of future injury to establish standing because it was plausible to infer that a party accessing plaintiffs' personal information did so with "both the intent and ability to use the data for ill."), *cert. denied*, 138 S. Ct. 981 (2018).

[35]*See Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384, 387-89 (6th Cir. 2016) (holding, by a 2-1 decision in an unreported opinion, that the plaintiffs had standing to sue based on the risk of future identity theft because "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals").

[36]*See, e.g.*, *Gordon v. Chipotle Mexican Grill, Inc.*, __ F. Supp. 3d __, 2018 WL 4620342 (D. Colo. 2018) (denying defendant's 12(b)(1) motion to dismiss for lack of standing and adopting in part the Magistrate Judge's ruling, finding a substantial risk of future harm that fraudulent accounts could be opened in the plaintiff's name), *adopting in part*, Civil Action No. 17-cv-1415-CMA-MLC, 2018 WL 3653173 (D. Colo. Aug 1, 2018) (Magistrate Judge recommendation, inferring from the allegations that additional personal information—beyond what was alleged—had been compromised by a security breach).

[37]*See Beck v. McDonald*, 848 F.3d 262 (4th Cir.) (holding that patients at a Veterans Affairs hospital who sued alleging that their personal information had been compromised as a result of two data breaches did not have standing because an enhanced risk of future identity theft was too speculative to cause injury in fact and the allegations were insufficient to establish a substantial risk of harm), *cert denied,* 137 S. Ct. 2307 (2017); *see also Hutton v. National Board of Examiners in Optometry, Inc.,* 243 F. Supp. 3d 609, 613-15 (D. Md. 2017) (following *Beck* in dismissing plaintiffs' claims under the California Customer Records Act, Cal. Civ. Code

the Second Circuit[39] in a non-precedential opinion, apply a more exacting standard that is arguably more consistent with the most recent U.S. Supreme Court case law on standing, as do the First[40] and Third[41] Circuits in older opinions

---

§§ 1798.81 *et seq*. and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, and for breach of contract, breach of implied contract, negligence and unjust enrichment, for lack of standing, where plaintiffs alleged that, as a result of a breach of a database containing PII from optometrists throughout the United States, they had incurred time and expenses (and, for one plaintiff, received a credit card that had not been requested, issued in the name she had used when she provided her PII to the defendant), because their assumption that the defendant suffered a data breach and was the source of the leaked data was based on online conversations, where plaintiffs "failed to allege a plausible, inferential link between the provision of PII to NBEO at some point in the past and their recent receipt of unsolicited credit cards.").

[38]*See In re SuperValu, Inc., Customer Data Security Breach Litig*., 870 F.3d 763 (8th Cir. 2017) (affirming dismissal of the claims of 15 of the 16 plaintiffs but holding that the one plaintiff who alleged that he had suffered a fraudulent charge on his credit card had standing to sue for negligence, breach of implied contract and unjust enrichment, among other claims).

[39]*See Whalen v. Michaels Stores, Inc.,* 689 F. App'x 89 (2d Cir. 2017) (affirming that the plaintiff lacked standing to sue for breach of implied contract and under N.Y. Gen. Bus. L. § 349 where she alleged that she made purchases via a credit card at a Michaels store on December 31, 2013, where Michaels experienced a breach involving credit card numbers but no other information such as a person's name, address or PIN, and where plaintiff alleged that her credit card was presented for unauthorized charges in Ecuador on January 14 and 15, 2014, but she did not allege that any fraudulent charges were actually incurred by her prior to the time she canceled her card on January 15 or that, before the cancellation, she was in any way liable on account of those presentations, and where she did not allege with any specificity that she spent time or money monitoring her credit).

[40]*See Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (holding that a brokerage account-holder's increased risk of unauthorized access and identity theft was insufficient to constitute "actual or impending injury" after the defendant failed to properly maintain an electronic platform containing her account information, because plaintiff failed to "identify any incident in which her data has ever been accessed by an unauthorized person").

[41]*See Reilly v. Ceridian Corp*., 664 F.3d 38, 40, 44 (3d Cir. 2011) (holding, in a carefully thought out opinion that contrasted security breach cases from other disputes involving standing, that employees' increased risk of identity theft was too hypothetical and speculative to establish "certainly impending" injury-in-fact after an unknown hacker penetrated a payroll system firewall, because it was "not known whether the hacker read, copied, or understood" the system's information and no evidence

that pre-date *Clapper*. It is likely that the U.S. Supreme Court will grant certiorari in an appropriate case to resolve this split of authority given the Roberts' Court's interest in issues of federal jurisdiction, including standing.

To better understand the current legal landscape and how it developed, it is helpful to take note of the circuit where a decision was rendered, and the date when it was issued. For context, this section addresses the chronological development of the law in this area, both before and following the U.S. Supreme Court's decisions in *Clapper v. Amnesty Int'l USA*[42] (which arguably tightened the standards for standing based on the threat of future injury) and *Spokeo, Inc. v. Robins*[43] (which addressed standing in cases where a plaintiff can state a claim under a federal statute that doesn't otherwise require a showing of injury).

It is also helpful to understand the procedural posture of a case when standing is raised.[44] A defendant may challenge subject-matter jurisdiction in one of two ways: facially or

---

suggested past or future misuse of employee data or that the "intrusion was intentional or malicious"), *cert. denied*, 566 U.S. 989 (2012).

While *Reilly* remains relevant for cases based on future harm, where a security breach claim is based on a federal statute, *Spokeo* may provide grounds for standing that would not otherwise exist for a common law claim. *See In re Horizon Healthcare Services Inc. Data Breach Litig.,* 846 F.3d 625, 629, 638–40 (3d Cir. 2017) (holding that plaintiffs had standing to sue for the disclosure of personal information, in violation of FCRA, as a result of the theft of two laptops, because of the statutory violation, and that the same facts would not necessarily "give rise to a cause of action under common law"; while also holding that "the 'intangible harm' that FCRA seeks to remedy 'has a close relationship to a harm [i.e., invasion of privacy] that has traditionally been regarded as providing a basis for a lawsuit in English or American courts,' *Spokeo*, 136 S. Ct. at 1549, . . . [and therefore] Congress properly defined an injury that 'give[s] rise to a case or controversy where none existed before.' ").

[42]*Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409-11 (2013) (holding that to establish Article III standing a plaintiff must allege an injury that is concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling). *Clapper* made clear that, to establish standing, a future injury must be "certainly impending," rather than speculative or based on "a highly attenuated chain of possibilities . . . ." *Id.* at 1148.

[43]*Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1547 (2016).

[44]*See Beck v. McDonald,* 848 F.3d 262, 270 (4th Cir.) (*citing Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) ("[E]ach element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation.")), *cert denied,*

factually.[45] At the pleading stage, injury may be shown by "general factual allegations of injury resulting from the defendant's conduct."[46] The appropriate standard is akin to one of general, rather than proximate causation.[47] Although a motion challenging standing at the outset of the case would be brought under Fed. R. Civ. Proc. 12(e) (for lack of subject matter jurisdiction), the plaintiff is "afforded the same procedural protection as she would receive under a Rule 12(b)(6)" motion to dismiss, where "the facts alleged in the complaint are taken as true . . . ."[48] Nevertheless, the requirement, even at the pleading stage, has been clarified to require a plaintiff to " 'clearly allege facts' demonstrating" the elements of standing.[49] The plaintiff must allege a basis for standing that is *plausible*.[50]

Standing alternatively may be challenged through affidavits or declarations. In a factual challenge, the defendant disputes plaintiff's allegations, affording the court discretion to "go beyond the allegations of the complaint and in an evidentiary hearing determine if there are facts to support the jurisdictional allegations."[51] "In this posture, 'the presumption of truthfulness normally accorded a complaint's allega-

---

137 S. Ct. 2307 (2017).

[45]*Beck v. McDonald,* 848 F.3d 262, 270 (4th Cir.) (*citing Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009)), *cert denied,* 137 S. Ct. 2307 (2017).

[46]*Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

[47]*See Attias v. Carefirst, Inc.,* 865 F.3d 620, 629 (D.C. Cir. 2017) ("Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be "fairly traceable" to the defendant."), *cert. denied*, 138 S. Ct. 981 (2018); *In re SuperValu, Inc., Customer Data Security Breach Litig*., 870 F.3d 763, 773 (8th Cir. 2017) (*citing Lexmark Int'l, Inc. v. Static Control Components, Inc.,*134 S. Ct. 1377, 1391 n.6 (2014) ("Proximate causation is not a requirement of Article III standing.")).

[48]*Beck v. McDonald,* 848 F.3d 262, 270 (4th Cir.) (quoting *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009), *cert denied*, 137 S. Ct. 2307 (2017); *see also In re Horizon Healthcare Services Inc. Data Breach Litig.,* 846 F.3d 625, 633 (3d Cir. 2017) ("In reviewing facial challenges to standing, we apply the same standard as on review of a motion to dismiss under Rule 12(b)(6).")), *cert denied,* 137 S. Ct. 2307 (2017).

[49]*Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1547 (2016), *quoting Warth v. Seldin,* 422 U.S. 490, 518 (1975).

[50]*Attias v. Carefirst, Inc.,* 865 F.3d 620, 625 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[51]*Beck v. McDonald,* 848 F.3d 262, 270 (4th Cir.) (quoting earlier

tions does not apply.' "[52]

As previously noted, most security breach suits where standing is an issue involve an actual security breach that has exposed some personal information, but individual harm may be absent, intangible, or merely *de minimis.* In addition to the risk of future harm, plaintiffs' counsel frequently argue that plaintiffs have standing based on the costs associated with mitigating that risk (if any) and/or the loss of value experienced by paying for a product or service that plaintiffs allege was over-priced based on the actual level of security provided.

In the past, plaintiffs' counsel often sought to bolster their clients' claims based on apprehension of a potential future harm by encouraging them to subscribe to credit monitoring services, alleging that the cost of credit monitoring was a present loss occasioned by the breach.[53] A number of courts, however, have rejected the notion that credit monitoring costs can confer standing where the threat that these costs address is itself viewed as speculative or at least not certainly impending.[54] As the U.S. Supreme Court explained

---

cases), *cert denied,* 137 S. Ct. 2307 (2017).

[52]*Beck v. McDonald,* 848 F.3d 262, 270 (4th Cir.) (quoting earlier cases), *cert denied,* 137 S. Ct. 2307 (2017).

[53]For this reason, companies that experience a security breach sometimes voluntarily offer affected consumers free credit monitoring services to deprive plaintiffs' counsel of a potential argument for standing to sue in litigation in federal court. *See generally infra* § 27.08[9] (analyzing state security breach notification laws that address credit monitoring). Connecticut and Delaware also may affirmatively require the provision of credit monitoring services in some instances. *See id.*

[54]*See, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011), *cert. denied*, 566 U.S. 989 (2012); *Beck v. McDonald*, 848 F.3d 262, 276-77 (4th Cir.) ("[S]elf-imposed harms cannot confer standing."), *cert denied*, 137 S. Ct. 2307 (2017); *In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 771 (8th Cir. 2017) ("[b]ecause plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury."); *In re U.S. Office of Personnel Management Data Security Breach Litig.*, 266 F. Supp. 3d 1, 36 (D.D.C. 2017) (holding that Federal employees did not have standing to sue over a cybersecurity breach by a contractor of the U.S. Office of Personnel Management; quoting *Clapper* for the proposition that "incurring 'certain costs as a reasonable reaction to a risk of harm' does not provide for injury if 'the harm [plaintiffs] seek to avoid is not certainly impending. . . . [R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypotheti-

in *Clapper v. Amnesty International USA*,[55] plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[56] The Seventh Circuit, however, held in one case (which was subsequently followed in an unreported Sixth Circuit opinion, but expressly rejected by the Fourth Circuit) that a company's decision to offer credit monitoring to customers following a security breach evidenced that the risk of harm was more than *de minimis* and therefore plaintiffs provided with credit monitoring services had Article III standing to sue over the security breach.[57] In a subsequent Seventh Circuit case, the court even found

---

cal future harm that is not certainly impending."); *Moyer v. Michael's Stores, Inc.,* No. 14 C 561, 2014 WL 3511500, at *4 (N.D. Ill. July 14, 2014); *In re SAIC Corp.*, 45 F. Supp. 3d 14, 26–27 (D.D.C. 2014); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 470–71 (D.N.J. 2013). As one court explained:

> The cost of guarding against a risk of harm constitutes an injury-in-fact only if the harm one seeks to avoid is a cognizable Article III injury. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1151 (2013). Therefore, the cost of precautionary measures such as buying identity theft protection provides standing only if the underling risk of identity theft is sufficiently imminent to constitute an injury-in-fact.

Moyer v. Michael's Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *4 n.1 (N.D. Ill. July 14, 2014). *But see In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1217 (N.D. Cal. 2014) (holding that where the court found that plaintiffs adequately alleged that they faced "a certainly impending future harm from the theft of their personal data, . . . the costs Plaintiffs . . . incurred to mitigate this future harm constitute an additional injury–in–fact.").

Moyer is no longer good law on the limited point about credit monitoring in light of the Seventh Circuit's subsequent ruling in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015), which is discussed later in this section. The case continues to be cited on other grounds.

[55]*Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013).

[56]*Clapper v. Amnesty International USA*, 568 U.S. 398, 402, 407 (2013) (rejecting respondents' alternative argument that they were suffering "present injury because the risk of . . . surveillance already has forced them to take costly and burdensome measures to protect the confidentiality of their international communications."). The Supreme Court explained that allowing plaintiffs to bring suit "based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of [their] first failed theory of standing." *Id.* at 416.

[57]*See Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015); *see also Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (adopting the same analysis in an unreported, 2-1 decision). *But see Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir.) (declining to follow *Remijas* on this point as inconsistent with

standing where the plaintiff had purchased credit monitoring services well before the breach but alleged that her decision to renew those services was largely based on the defendant's security breach.[58] These rulings, which are discussed further later in this section, have left companies perplexed about how to respond when there has been a security breach.[59]

While credit monitoring alternatively has been seen as a

Clapper; "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. To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit."), *cert denied*, 137 S. Ct. 2307 (2017).

[58]*See Dieffenbach v. Barnes & Noble, Inc.,* 887 F.3d 826, 827-30 (7th Cir. 2018) (holding that one of the two plaintiffs had stated a claim for damages because the plaintiff had standing to assert Illinois state law claims against a merchant for a security breach arising out of compromised PIN pads used to verify credit card information, where the plaintiff alleged that (1) her bank contacted her about a potentially fraudulent charge on her credit card statement and deactivated her card for several days, and (2) the security breach at Barnes & Noble "was a decisive factor" when she renewed a credit-monitoring service for $16.99 per month).

[59]Connecticut and Delaware require companies to provide credit monitoring services in certain instances in response to a security breach. *See infra* § 27.08[9]. Where credit monitoring can mitigate the risk of identity theft, it should be considered a best practice to provide credit monitoring services free of charge to consumers, even where it is not legally required, with an explanation about the actual risks associated with identity theft so that the mere act of providing credit monitoring is not seen as an admission of harm. Credit monitoring, after all, is frequently offered simply to put customers at ease and maintain goodwill.

Any notice sent to consumers following a breach should not mislead consumers about the risks involved. Underplaying the risks, could leave a business exposed to negligence or other claims.

At the same time, companies should be cautious about issuing boilerplate warnings. In *Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963 (7th Cir. 2016), for example, the Seventh Circuit held that plaintiff's established standing to sue based on a concrete threat of identity theft where only debit card information had been compromised. Although the defendant argued—correctly—that this security breach did not create a risk of identity theft (only a risk of unauthorized charges on the accounts that were exposed, if the accounts were not cancelled), the fact that the defendant warned its customers to check their credit reports, in connection with announcing the breach, was cited as evidence that the breach could result in identity theft. *See id.* at 967-68.

Similarly, in *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023-30 (9th Cir. 2018), the Ninth Circuit cited a routine, boilerplate warning that users should change their passwords, following a security breach, as evi-

panacea for both plaintiff's and defense counsel in different cases, in the battle over standing, it in fact only provides a useful service for certain types of breaches. Where personal information has been exposed, there may be a risk that a third party could engage in identity theft by using the person's name and other information to open new credit accounts in the victim's name. For example, with a person's name, address, and Social Security Number, a person potentially could open a bank account or apply for a new credit card, lease or purchase a car, or seek a loan. Where only a credit card has been exposed, the only thing a hacker can do is attempt to make unauthorized charges on the account until it is cancelled; the information would not allow the hacker to steal a person's identity. Credit monitoring therefore may not actually remedy a harm in all instances when there has been a security breach. Courts nevertheless only rarely analyze credit monitoring in this granular way.

The divergence of opinions over whether providing credit monitoring services can help defeat or establish standing—or is irrelevant to the analysis—underscores that there have been a number of twists and turns in the law governing standing in security breach cases over the past several years. It is therefore important to understand trends in the law and circuit splits that may not be apparent if you simply line up cases and try to distinguish them based only on their facts.

As outlined below, prior to the U.S. Supreme Court's 5-4 decision in *Clapper v. Amnesty International USA*,[60] there was a split in the Circuits on whether standing could be established in a security breach case where there was no present injury. *Clapper* addressed squarely the issue of standing premised on the threat of future harm and generally has been construed to have tightened the standards for standing in security breach cases, except in the Seventh and Ninth Circuits (and opinions applying Seventh Circuit law in the Sixth and D.C. Circuits), which have continued to construe the requirements for standing in security breach cases based on the threat of future harm more liberally, con-

---

dence of the severity of the breach, which supported the Ninth Circuit's finding of standing in that case.

These opinions create a perverse disincentive for businesses to issue normal precautionary warnings and suggest, at a minimum, that the wording used in notices to consumers should be chosen carefully.

[60] *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013).

sistent with pre-*Clapper* precedents from the Seventh and Ninth circuits. The Supreme Court's subsequent 6-2 compromise decision in *Spokeo, Inc. v. Robins*,[61] which occurred following the death of conservative Justice Antonin Scalia in early 2016, adds yet another new standard for courts to evaluate in cases where standing is premised on breach of a federal statute.

Standing in Putative Cybersecurity Breach Consumer Class Action Suits—In Depth and in Chronological Context

Prior to *Clapper*, the Seventh[62] and Ninth[63] Circuits and

---

[61]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[62]*Pisciotta v. Old National Bancorp.*, 499 F.3d 629 (7th Cir. 2007) (finding standing in a security breach class action suit against a bank, based on the threat of future harm from an intrusion that was "sophisticated, intentional and malicious."). In *Pisciotta,* plaintiffs sued a bank after its website had been hacked, alleging that it failed to adequately secure the personal information that it had solicited (including names, addresses, birthdates and Social Security numbers) when customers had applied for banking services on its website. Plaintiffs did not allege that they had yet incurred any financial loss or been victims of identity theft. Rather, the court held that they satisfied the "injury in fact" requirement to establish standing based on the threat of future harm or "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." *Id.* at 634.

[63]*Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010) (finding standing in a suit where plaintiffs' unencrypted information (names, addresses and Social Security numbers) was stored on a stolen laptop, where someone had attempted to open a bank account with plaintiff's information following the theft, creating "a credible threat of real and immediate harm stemming from the theft . . . ."); *see also Doe I v. AOL*, 719 F. Supp. 2d 1102, 1109–11 (N.D. Cal. 2010) (finding injury in fact, in a case pre-dating *Krottner*, where a database of search queries was posted online containing AOL members' names, social security numbers, addresses, telephone numbers, user names, passwords, and bank account information, which could be matched to specific AOL members); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908 (N.D. Cal. 2009) (holding, prior to *Krottner,* that a job applicant whose personal information (including his Social Security number) had been stored on a laptop of the defendant's that had been stolen had standing to sue but granting summary judgment for the defendant where the risk of future identity theft did not support claims for negligence, breach of contract, unfair competition or invasion of privacy under the California constitution), *aff'd mem.,* 380 F. App'x 689 (9th Cir. 2010). *But see In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (dismissing plaintiffs' putative class action suit arising out of a hacker gaining access to their LinkedIn passwords and email addresses, for lack of Article III standing, where plaintiffs alleged no injury or damage).

district courts elsewhere[64] applied a more liberal standard and generally held that consumers impacted by security breaches where data had been accessed by unauthorized third parties, but no loss had yet occurred, had standing to maintain suit in federal court based on the threat of future harm, while the Third Circuit, in a better reasoned, more detailed analysis, disagreed[65] (and various district courts (both before and after *Clapper*)[66] have similarly found the

---

[64]*See, e.g., Holmes v. Countrywide Financial Corp.,* No. 5:08-CV-00205-R, 2012 WL 2873892, at *5 (W.D. Ky. July 12, 2012) (holding that plaintiffs had standing to maintain suit over the theft of sensitive personal and financial customer data by a Countrywide employee where plaintiffs had purchased credit monitoring services to ensure that they would not be the targets of identity thieves or expended sums to change their telephone numbers as a result of increased solicitations); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273 (S.D.N.Y. 2008) (holding that the plaintiff had standing to sue his employer's pension consultant, seeking to recover the costs of multi-year credit monitoring and identity theft insurance, following the theft of a laptop containing his personal information from the consultant's office).

[65]*Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (finding no standing in a suit by law firm employees against a payroll processing firm alleging negligence and breach of contract relating to the risk of identity theft and costs for credit monitoring services in a case where defendant's firewall had been penetrated but there was no evidence that the intrusion was intentional or malicious and no allegation of misuse and therefore injury), *cert. denied,* 566 U.S. 989 (2012); *see also Allison v. Aetna, Inc.,* No. 09–2560, 2010 WL 3719243, at *5 n.7 (E.D. Pa. Mar. 9, 2010) (pre-*Ceridian* district court case rejecting claims for negligence, breach of express and implied contract and invasion of privacy, for time and money spent on credit monitoring due to a perceived risk of harm as the basis for an injury in fact, in a case where the plaintiff did not allege any harm as a result of a job application website breach of security); *Hinton v. Heartland Payment Systems, Inc.,* Civil Action No. 09–594 (MLC), 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (pre-*Ceridian* opinion, dismissing the case *sua sponte* because plaintiff's allegations of increased risk of identity theft and fraud "amount to nothing more than mere speculation."); *Giordano v. Wachovia Securities, LLC,* No. 06 Civ. 476, 2006 WL 2177036, at *5 (D.N.J. July 31, 2006) (pre-*Ceridian* district court case holding that credit monitoring costs resulting from lost financial information did not constitute an injury sufficient to confer standing).

[66]*See, e.g., Antman v. Uber Technologies, Inc.*, Case No. 3:15-cv-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018) (dismissing, with prejudice, plaintiff's claims, arising out of a security breach, for allegedly (1) failing to implement and maintain reasonable security procedures to protect Uber drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3)

negligence; and (4) breach of implied contract, for lack of Article III standing, where plaintiff could not allege injury sufficient to establish Article III standing); *Patton v. Experian Data Corp.*, No. SACV 15-1871 JVS (PLAx), 2016 WL 2626801, at *4 (C.D. Cal. May 6, 2016) (rejecting the increased risk of identity theft as a basis for standing because any harm depended on a series of facts that were not alleged: (1) that an identity thief accessed their personal information; (2) that an identity thief provided their personal information to any third-parties; and (3) that any person had unlawfully used personal information of theirs that had been stored in Experian's database); *Alonso v. Blue Sky Resorts, LLC*, 179 F. Supp. 3d 857 (S.D. Ind. 2016) (holding that guests did not have standing to sue a hotel over a security breach), *appeal dismissed*, Appeal No. 16-2136 (7th Cir. Jan. 10, 2017); *In re SuperValu, Inc., Customer Data Security Breach Litig.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792 (D. Minn. Jan. 7, 2016) (rejecting standing under an array of theories), *aff'd in part*, 870 F.3d 763 (8th Cir. 2017) (affirming dismissal of the claims of 15 of the 16 plaintiffs but holding that the one plaintiff who alleged he suffered a fraudulent charge on his credit card had standing to sue for negligence, breach of implied contract and unjust enrichment, among other claims); *Whalen v. Michael Stores Inc.*, 14-CV-7006 (JS)(ARL), 2015 WL 9462108 (E.D.N.Y. Dec. 28, 2015) (dismissing plaintiff's breach of implied contract and N.Y. Gen. Bus. L. § 349 claims for lack of standing in a case arising out of a security breach where a credit card was used but there was no allegation that the plaintiff bore the risk of loss), *aff'd*, 689 F. App'x 89 (2d Cir. 2017); *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955, 973 (N.D. Cal. 2015) (holding that plaintiffs lacked standing because geographic location information could not plausibly "establish any credible risk of future harm"), *aff'd*, 717 F. App'x 720 (9th Cir. 2017); *Foster v. Essex Property Trust, Inc.,* Case No. 5:14-cv-05531-EJD, 2015 WL 7566811 (N.D. Cal. Nov. 25, 2015) (dismissing plaintiff's claim for lack of standing in a case involving information stolen from the defendant's computer system); *Antman v. Uber Technologies, Inc.*, No. 3:15-cv-01175, 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015) (holding that the risk that plaintiff's identity could be stolen was insufficient to confer standing based on a data breach exposing plaintiff's name and driver's license number because that information, standing alone, could not be used to steal money or an identity); *Green v. eBay, Inc.*, Civil No. 14–1688, 2015 WL 2066531 (E.D. La. May 4, 2015); *Peters v. St. Joseph Services Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015) (holding that the alleged increased risk of future identity theft or fraud was not a cognizable Article III injury and even the allegation of actual identity theft or fraud was insufficient to establish standing in the absence of any injury); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) (holding that, under *Clapper*, a plaintiff failed to allege an imminent injury as a result of a data breach, because the plaintiff did not allege a "basis to believe that" any of the "number of variables" required for her identity to be stolen had "come to pass or are imminent," and the harm that the plaintiff "fears [was] contingent upon a chain of attenuated hypothetical events and actions by third parties independent of the defendant"); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1092–95 (N.D. Cal. 2013) (dismissing plaintiffs' putative class action suit arising out of a hacker gaining access to their LinkedIn passwords and

threat of future harm to be too speculative to support standing based on the facts alleged in particular cases).

In *Reilly v. Ceridian Corp.*,[67] the Third Circuit rejected the analogy drawn by the Seventh and Ninth Circuits between data security breach cases and defective-medical-device, toxic-substance-exposure or environmental injury cases,

---

email addresses, for lack of standing, where plaintiffs failed to allege any present harm and their allegations of possible future harm were "too theoretical to support injury-in-fact for the purposes of Article III standing."); *Whitaker v. Health Net of California, Inc.,* No. 11-910, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012) (granting IBM's motion to dismiss for lack of standing where plaintiffs did "not explain how the loss here has actually harmed them . . . or that third parties have accessed their data. Any harm stemming from their loss thus is precisely the type of conjectural and hypothetical harm that is insufficient to allege standing."); *Hammond v. Bank of N.Y. Mellon Corp.,* No. 08–6060, 2010 WL 2643307, at *4, *7 (S.D.N.Y. June 25, 2010) (finding no standing and, in the alternative, granting summary judgment on plaintiff's claims for negligence, breach of fiduciary duty, implied contract and state consumer protection violations based, among other things, on the absence of any injury); *Allison v. Aetna, Inc.,* 09–CV–2560, 2010 WL 3719243 (E.D. Pa. Mar. 9, 2010) (finding no standing based solely on the increased risk of identity theft); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1051–53 (E.D. Mo. 2009) (dismissing claims for negligence, breach of contract with respect to third-party beneficiaries, breach of implied contract, violations of various states' data breach notification laws, and violations of Missouri's Merchandising Practices Act, arising out of an alleged database security breach, because the increased risk of future identity theft was insufficient to confer standing and for failure to state a claim); *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705 (S.D. Ohio 2007) (granting defendant's motion for summary judgment in a suit for negligence, arising out of the theft of a mortgage loan service provider's computer equipment, where the plaintiff could not establish injury or causation); *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1 (D.D.C. 2007) (holding that plaintiffs lacked standing to sue their insurer for public disclosure of private facts, negligence, gross negligence or breach of fiduciary duty after a laptop containing their private personal information was stolen, where plaintiffs' alleged increased risk of identity theft and the costs incurred to protect themselves against that alleged increased risk did not amount to injury in fact sufficient for standing); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 688–90 (S.D. Ohio 2006) (dismissing a putative class action suit alleging negligence, breach of contract, conversion, and breach of fiduciary duty, for lack of standing, where a security breach allowed unauthorized persons to obtain access to personal financial information of approximately 96,000 customers but the breach created "only the possibility of harm at a future date."); *Bell v. Acxiom Corp.,* No. 4:06 Civ. 00485, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (finding no standing where plaintiff pled only an increased risk of identity theft rather than "concrete damages.").

[67] *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012).

where courts typically find standing.

First, in those cases, an injury "has undoubtedly occurred" and damage has been done, even if the plaintiffs "cannot yet quantify how it will manifest itself."[68] In data breach cases where no misuse is alleged, however, "there has been no injury—indeed, no change in the status quo . . . . [T]here is no quantifiable risk of damage in the future . . . . Any damages that may occur . . . are entirely speculative and dependent on the skill and intent of the hacker."[69]

Second, standing in medical-device and toxic-tort cases "hinges on human health concerns" where courts resist strictly applying the "actual injury" test "when the future harm involves human suffering or premature death."[70] Similarly, standing in environmental injury cases is unique "because monetary compensation may not adequately return plaintiffs to their original position."[71] By contrast, in a data breach case, "there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely—*if* the hacked information is actually read, copied, understood, and misused to a plaintiff's detriment. To the contrary, . . . the thing feared lost . . . is simply cash, which is easily and precisely compensable with a monetary award."[72]

In *Ceridian,* the Third Circuit also rejected the argument that time and money spent to monitor plaintiffs' financial information established standing because "costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the

---

[68]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012).

[69]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012). As the court explained, in *Reilly* "Appellant's credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked." *Id.*

[70]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012).

[71]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012).

[72]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45–46 (3d Cir. 2011) (emphasis in original), *cert. denied,* 566 U.S. 989 (2012).

basis for Appellants' claims."[73]

While there was a split of authority in these cases (as noted above), the argument for standing in a lawsuit based on the mere threat of a potential security breach, without even evidence of present injury, was weak. In *Katz v. Pershing, LLC,*[74] the First Circuit distinguished both the Third Circuit's holding in *Ceridian*[75] and Seventh and Ninth Circuit opinions finding standing in data breach suits,[76] in a putative class action suit in which the plaintiff had sued based on an increased risk that someone *might* access her data, rather than an actual security breach. The court held that plaintiff's allegations—which it characterized as "unanchored to any actual incident of data breach"—were too remote to support Article III standing.[77]

Similarly, in *Frezza v. Google Inc.*,[78] a district court case, the court, in dismissing a breach of implied contract claim

---

[73]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012).

[74]*Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012).

[75]*Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012).

[76]*Pisciotta v. Old National Bancorp.*, 499 F.3d 629 (7th Cir. 2007); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).

[77]*Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (holding that the plaintiff did not have Article III standing to sue the defendant for failing to provide notice pursuant to Massachusetts' security breach notification law where "the plaintiff purchased identity theft insurance and credit monitoring services to guard against a possibility, remote at best, that her nonpublic personal information might someday be pilfered. Such a purely theoretical possibility simply does not rise to the level of a reasonably impending threat."). In *Katz,* the First Circuit emphasized that

> the plaintiff has not alleged that her nonpublic personal information actually has been accessed by any unauthorized person. Her cause of action rests entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity. The conjectural nature of this hypothesis renders the plaintiff's case readily distinguishable from cases in which confidential data actually has been accessed through a security breach and persons involved in that breach have acted on the ill-gotten information. *Cf. Anderson v. Hannaford Bros.,* 659 F.3d 151, 164–65 (1st Cir. 2011) (holding purchase of identity theft insurance in such circumstances reasonable in negligence context). Given the multiple strands of speculation and surmise from which the plaintiff's hypothesis is woven, finding standing in this case would stretch the injury requirement past its breaking point.

Katz v. Pershing, LLC, 672 F.3d 64, 79–80 (1st Cir. 2012).

[78]*Frezza v. Google Inc.,* No. 5:12-cv-00237, 2013 WL 1736788 (N.D. Cal. Apr. 22, 2013).

brought over Google's alleged failure to implement Data Security Standards (DSS) rules in connection with promotions for Google Tags, distinguished cases where courts found standing involving the disclosure of personal information, as opposed to mere retention of data, which was what was alleged in *Frezza*.

In 2013, the U.S Supreme Court, in *Clapper v. Amnesty International USA*,[79] emphasized that to establish standing "allegations of possible future injury are not sufficient."[80] The threatened injury must be "certainly impending" to constitute injury in fact.[81] In *Clapper,* the Supreme Court held that U.S.-based attorneys, human rights, labor, legal and media organizations did not have standing to challenge section 702 of the Foreign Intelligence Surveillance Act of 1978,[82] based on their allegation that their communications with individuals outside the United States who were likely to be the targets of surveillance under section 702 made it likely that their communications would be intercepted. The Court characterized their fear as "highly speculative" given that the respondents did not allege that any of their communications had actually been intercepted, or even that the U.S. Government sought to target them directly.[83]

Clapper arguably made it even more difficult for plaintiffs in security breach cases to establish standing in federal court in the absence of identity theft. Indeed, courts in many data security cases have read *Clapper* this way.[84] As one court observed after *Clapper*, under current pleading standards it

---

[79]*Clapper v. Amnesty International USA*, 568 U.S. 398 (2013).

[80]*Clapper v. Amnesty International USA*, 68 U.S. 398, 409 (2013) (internal quotation marks omitted).

[81]*Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013).

[82]50 U.S.C.A. § 1881a.

[83]*Clapper v. Amnesty International USA*, 568 U.S. 398, 410 (2013).

[84]*See, e.g., Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1286 (N.D. Ala. 2014) (dismissing plaintiff's negligence claim with leave to amend, citing cases that applied *Clapper* but not *Clapper* itself); *In re SAIC Corp.*, 45 F. Supp. 3d 14 (D.D.C. 2014) (dismissing claims brought on behalf of 4.7 million military members and their families whose data was exposed by a government contractor, but allowing a few very specific claims where actual loss was alleged to proceed); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 467–71 (D.N.J. 2013) (relying on *Clapper* and *Reilly* to conclude that the mere loss of data, without misuse, is not a sufficient injury to confer standing); *In re Barnes & Noble Pin Pad Litig.,* 12-CV-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (rejecting arguments that the delay or inadequacy of breach notification increased the

may be "difficult for consumers . . . to assert a viable cause of action stemming from a data breach because in the early stages of the 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."[85]

Courts in some jurisdictions that previously had more permissive standing rules, however, have applied more liberal standing requirements to security breach cases, consistent with pre-*Clapper* circuit court law.

In *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[86] a court in San Diego reiterated, in January 2014, its earlier ruling finding that plaintiffs in a security breach case had standing, which had been decided before *Clapper*, based on *Krottner v. Starbucks Corp*.,[87] the leading pre-*Clapper* Ninth Circuit security breach standing case. In *Sony,* Judge Anthony Battaglia concluded that *Krottner* remained binding precedent and was not inconsistent with *Clapper*. He wrote that "although the Supreme Court's word choice in *Clapper* differed from the Ninth Circuit's word choice in *Krottner*, stating that the harm must be 'certainly impending,' rather than 'real and immediate,' the Supreme Court's decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be 'real and immediate.' "[88]

Thereafter, in September 2014, in what at first appeared to be an aberrational opinion that eventually proved influen-

---

risk of injury and, citing *Clapper*, explaining that "[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing."); *see also Yunker v. Pandora Media, Inc.*, No. 11–3113, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) (holding, in a privacy case, that plaintiff lacked standing to sue under *Clapper* based on theories that (1) Pandora's conduct diminished the value of his personally identifiable information ("PII"); (2) Pandora's conduct decreased the memory space on his mobile device; and (3) Pandora's disclosure of his PII put him at risk of future harm, but holding that the plaintiff had standing to sue based on the theory that Pandora invaded his constitutional right to privacy when it allegedly disseminated his PII to third parties).

[85]*Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1280 (N.D. Ala. 2014).

[86]*In re Sony Gaming Networks & Customer Data Security Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014).

[87]*Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010).

[88]*In re Sony Gaming Networks & Customer Data Security Breach Litig.*, 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014).

tial, Northern District of California Judge Lucy Koh ruled in *In re Adobe Systems, Inc. Privacy Litigation*[89] that plaintiffs whose information had been compromised but who had not been victims of identity theft had standing to bring a putative class action suit based on pre-*Clapper* Ninth Circuit law.

In *Adobe,* Judge Koh held that plaintiffs had standing to assert claims for declaratory relief and under Cal. Civil Code § 1798.81.5 for Adobe's alleged failure to maintain reasonable security for their data and for unfair competition for failing to warn about allegedly inadequate security in connection with a security breach that exposed the user names, passwords, credit and debit card numbers, expiration dates, and email addresses of 38 million customers. At the same time, she dismissed plaintiffs' claims for allegedly delaying consumer breach notification where there was no traceable harm and plaintiffs' claim that they had spent more money on Adobe products than they would have had they known the true level of security provided by the company.

Judge Koh wrote that "*Clapper* did not change the law governing Article III standing" because the U.S. Supreme Court did not overrule any of its prior precedents and did not "reformulate the familiar standing requirements of injury-in-fact, causation and redressability." Accordingly, Judge Koh expressed reluctance to construe *Clapper* broadly as expanding the standing doctrine.

Judge Koh also distinguished *Clapper* because in that case standing arose in the sensitive context of a claim that "other branches of government in that case were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result."[90] She explained:

> "[D]istrict courts should consider themselves bound by . . . intervening higher authority and reject the prior opinion of [the Ninth Circuit] as having been effectively overruled" only

---

[89] *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

[90] *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014), *citing Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013) ("Our standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." (alteration omitted) (internal quotation marks omitted).

> when the intervening higher authority is "clearly irreconcilable with [the] prior circuit authority." *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). The Court does not find that *Krottner* and *Clapper* are clearly irreconcilable. *Krottner* did use somewhat different phrases to describe the degree of imminence a plaintiff must allege in order to have standing based on a threat of injury, *i.e.*, "immediate[ ][ ] danger of sustaining some direct injury," and a "credible threat of real and immediate harm." 628 F.3d at 1142–43. On the other hand, *Clapper* described the harm as "certainly impending." 133 S. Ct. at 1147. However, this difference in wording is not substantial. At the least, the Court finds that *Krottner* 's phrasing is closer to *Clapper* 's "certainly impending" language than it is to the Second Circuit's "objective reasonable likelihood" standard that the Supreme Court reversed in *Clapper*. Given that *Krottner* described the imminence standard in terms similar to those used in *Clapper*, and in light of the fact that nothing in *Clapper* reveals an intent to alter established standing principles, the Court cannot conclude that *Krottner* has been effectively overruled.[91]

In the alternative, she ruled that even if *Krottner v. Starbucks Corp*.[92] was "no longer good law, the threatened harm alleged . . . [in *Adobe* was] sufficiently concrete and imminent to satisfy *Clapper*."[93] Unlike in *Clapper*, Judge Koh wrote, where respondents' claim that they would suffer future harm rested on a chain of events that was both "highly attenuated" and "highly speculative," the risk that plaintiffs' personal data in *Adobe* would be misused by the hackers who breached Adobe's network was "immediate and very real" because plaintiffs alleged that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates and plaintiffs' personal information was among the information taken during the breach. "Thus, in contrast to *Clapper*, where there was no evidence that any of respondents' communications either had been or would be monitored under Section 702, . . . [in *Adobe* there was] no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken. Neither is there any need to speculate as to whether the hackers intend

---

[91] *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014).

[92] *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010).

[93] *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014).

to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so."[94] In so ruling, Judge Koh distinguished *Polanco v. Omnicell, Inc.*,[95] as a case involving the theft of a laptop from a car where there was no allegation that the thief targeted the laptop for the data stored on it, and *Strautins v. Trustware Holdings, Inc.*[96] and *In re Barnes & Noble Pin Pad Litigation,*[97] as cases where it was not clear that any data was stolen at all.

By contrast, Judge Koh disagreed with *Galaria v. Nationwide Mutual Insurance Co.,*[98] which she characterized as the most factually similar of the cases she discussed, taking issue with the court's conclusion in that case that "whether plaintiffs would be harmed depended on the decision of the unknown hackers, who may or may not attempt to misuse the stolen information."[99] Judge Koh characterized this reasoning as unpersuasive and declined to follow it, asking rhetorically, "why would hackers target and steal personal customer data if not to misuse it? . . . ."[100] Regardless, she wrote, *Galaria*'s reasoning lacked force in *Adobe,* where plaintiffs alleged that some of the stolen data already had been misused.

In a footnote, Judge Koh further noted that "requiring Plaintiffs to wait for the threatened harm to materialize in order to sue would pose a standing problem of its own, because the more time that passes between a data breach

---

[94]*In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014).

[95]*Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 456 (D.N.J. 2013).

[96]*Strautins v. Trustware Holdings, Inc.*, 27 F. Supp. 3d 871 (N.D. Ill. 2014).

[97]*In re Barnes & Noble Pin Pad Litig.*, No. 12 C 8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013). In connection with a subsequent, Second Amended Complaint, the Seventh Circuit held that the plaintiffs had stated a claim for damage because they had Article III standing. *See Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 827-30 (7th Cir. 2018).

[98]*Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014), *rev'd*, 663 F. App'x 384 (6th Cir. 2016). As discussed later in this section, Judge Koh's ruling proved influential in subsequent Seventh Circuit opinions addressing standing in security breach cases, which in turn influenced the majority of the Sixth Circuit panel, on appeal, to reverse the district court's ruling finding no standing in *Galaria*.

[99]*In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014).

[100]*In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014).

and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."[101]

Judge Koh's analysis proved influential in *Remijas v. Neiman Marcus Group, LLC*,[102] in which the Seventh Circuit, in an opinion written by Chief Judge Wood, reversed the district court, holding that the plaintiffs in that case plausibly alleged standing. The security breach at issue in that case was the same one that had affected Target in late 2013. On January 10, 2014, Neiman Marcus announced that a cyberattack had occurred between July 16, 2013 and October 30, 2013, exposing approximately 350,000 credit cards. The district court had dismissed plaintiffs' claim as too speculative.

On appeal, the Seventh Circuit panel emphasized that the personal data of all putative class members had been stolen and 9,200 people had already incurred fraudulent charges. Although these people had been reimbursed for the charges, the appellate panel emphasized that there were "identifiable costs associated with the process of sorting things out."[103]

Relying on *Adobe* and Judge Koh's interpretation of *Clapper,* the Seventh Circuit held that it was plausible to infer that the plaintiffs had shown a substantial risk of harm from the data breach. The panel surmised that hackers would not break into a store's database and steal personal information if they did not actually intend to make use of it "sooner or later . . . ."[104]

In addition to future injuries, the appellate panel credited plaintiffs' assertion that they had already lost time and money protecting themselves against future identity theft. Citing *Clapper,* the panel acknowledged that mitigation expenses do not qualify as actual injuries when the harm is not imminent, but unlike in *Clapper*, where the alleged harm was speculative, in *Remijas,* the panel explained, the threat

---

[101] *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014).

[102] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015).

[103] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692 (7th Cir. 2015).

[104] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015). It is not clear that this assumption is correct. When credit card information is stolen it is most valuable initially before consumers and their credit card companies cancel the accounts and issue new cards.

was more imminent. In this regard, the fact that Neiman Marcus had offered a year of free credit monitoring services to plaintiffs was viewed by the Seventh Circuit panel as evidence that the threat of future harm was real and the cost of identity theft protection (even though borne by Neiman Marcus) was "more than *de minimis*."[105] Ironically, credit monitoring services are often provided by companies that have experienced a security breach as a litigation tactic to minimize the risk that putative class members would be able to establish standing through mitigation expenses, or to build consumer goodwill in the face of a breach, or as required under state law.[106]

The court's assumption that a company's voluntary provision of credit monitoring services evidences the severity of the breach for purposes of Article III standing is unjustified. Many companies in the past offered credit monitoring services following a breach in the interest of good customer relations and to deter litigation, not because of the risk of harm. Moreover, there is a fundamental difference between a prophylactic measure taken to prevent a risk of harm, however small, and the magnitude of the risk mitigated—which may be a function of the severity of the consequences of the risk more than the likelihood that it will come to pass. There is simply no basis to extrapolate the degree of risk of identity theft from a company's willingness to undertake the relatively small cost of providing credit monitoring services (compared to the cost of litigation, let alone liability). It is the legal equivalent of saying that a person's decision to have an annual physical exam evidences that they had a more than *de minimis* chance of dying that year. This kind of false calculation of risk based on preventative measures taken sets a very low bar for standing given that almost everyone in America today has had information exposed in a security breach (and more typically, in multiple security breaches), but only a small percentage have actually been victims of identity theft as a result of a breach. The Seventh Circuit's assumption—that provision of credit monitoring services evidences a serious risk of identity theft—creates a perverse disincentive for companies to provide credit moni-

---

[105] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015).

[106] *See infra* § 27.08[9] (discussing identity theft mitigation and prevention services, including credit monitoring, in connection with compliance with state security breach notification laws).

toring in instances where it could help consumers deter identity theft, out of concern that doing so could increase a company's potential exposure in litigation. For this reason, other circuits have declined to draw this same inference[107] (or even accept that a *plaintiff's* decision to purchase credit monitoring reflects actual harm if the risk mitigated is not sufficient to establish injury in fact).[108]

The Seventh Circuit's other assumption—that standing could be justified because a hacker wouldn't have stolen information if they didn't intend to use it—likewise is unjustified. It assumes that neither consumers nor credit card issuers, banks or others can do anything to prevent financial loss once information has been compromised, when in fact in many breaches most affected credit cards are cancelled before a consumer even knows that his or her credit card has been compromised. A thief's intent or determination in most cases is a poor predictor of whether compromised information will result in identity theft or some other financial loss.

While the Seventh Circuit broadly recognized that even people who have not been victims of identity theft may have standing where a breach, by its nature, suggests that the plaintiffs were targeted for their information, or that it was likely to be used, the appellate panel declined to address two of the plaintiffs' more aggressive theories of standing. Plaintiffs had argued that their actual expenditures with Neiman Marcus included a portion of money that should have been dedicated to securing their information and, because it was not, represented a premium to the company that amounted to a loss to the putative class. The plaintiffs also argued that their personal information has resale value and that by virtue of the security breach that value has been

---

[107] *See Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir.) (footnote omitted), *cert denied*, 137 S. Ct. 2307 (2017). *Beck* is discussed later in this section.

[108] *See In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 771 (8th Cir. 2017) ("Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.") (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 402 (2013) (holding that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending")); and *Beck v. McDonald*, 848 F.3d 262, 276-77 (4th Cir.) ("[S]elf-imposed harms cannot confer standing."), *cert denied*, 137 S. Ct. 2307 (2017). *SuperValu* is discussed later in this section.

diminished, which the panel characterized "some form of unjust enrichment . . . ."[109]

Remijas ultimately should be seen as a decision that is consistent with pre-*Clapper* Seventh Circuit case law, which similarly set a very low bar for standing.[110] It nevertheless had a significant impact on subsequent courts because it was the first data breach standing case decided by a Circuit Court since *Clapper*. Indeed, before any other circuit could weigh in, the Seventh Circuit, in early 2016, decided *Lewert v. P.F. Chang's China Bistro Inc.*,[111] in which—as in *Remijas*—it also reversed a lower court decision in a security breach case dismissing a lawsuit based on lack of Article III standing under *Clapper*.

In *Lewert,* the Seventh Circuit, in an opinion again written by Chief Judge Wood, held that at least some of the injuries that the two plaintiffs, Lewert and Kosner, alleged, were sufficiently "immediate and concrete" to support Article III standing under *Remijas*.[112] In that case, the plaintiffs had eaten at P.F. Chang restaurants and provided their debit cards to pay for their meals. Although P.F. Chang's initially announced that its computer system had been attacked and credit card information exposed, it later determined that the restaurant where the plaintiffs had eaten was not one from which debit card numbers had been compromised. Nevertheless, plaintiff Kosner alleged that fraudulent charges were attempted on his debit card, which he subsequently cancelled. Even though he incurred no costs himself, he purchased credit monitoring services for $106.89. Plaintiff Lewert neither purchased credit monitoring services nor cancelled his debit card. Both plaintiffs nevertheless alleged that they incurred time and expenses associated with the breach.

In holding that the plaintiffs had established Article III standing, Judge Wood identified both future and present

---

[109]*Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 695 (7th Cir. 2015).

[110]*See, e.g., Pisciotta v. Old National Bancorp.,* 499 F.3d 629 (7th Cir. 2007) (finding standing in a security breach class action suit against a bank based on the threat of future harm).

[111]*Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963 (7th Cir. 2016).

[112]*Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963, 967-69 (7th Cir. 2016).

injuries that justified standing under *Remijas.* The future injuries included the increased risk of fraudulent charges (for Lewert, who never cancelled his debit card) and identity theft. The present injuries included both plaintiffs spending time and effort monitoring financial statements. In addition, because fraudulent charges were attempted on Kosner's card, he spent time and effort, even if he incurred "no injury to his wallet (. . . his bank stopped the charges before they went through) . . . ."[113]

In so ruling, the Seventh Circuit rejected the argument that, unlike in *Remijas,* the P.F. Chang's security breach posed no risk of identity theft because only debit card information, not personal information that could be used to open new accounts in plaintiffs' names or otherwise engage in identity theft, was compromised.[114] Even though this argument is factually accurate, the court did not credit it because P.F. Chang's itself, in its press release announcing the breach, encouraged consumers to monitor their credit reports for new account activity, rather than simply reviewing their statements for the cards that were compromised.[115] *P.F. Chang's* thus underscores the importance of choosing words carefully in issuing public statements when a breach occurs.

Judge Wood also rejected the argument that plaintiffs lacked standing because it turned out that the plaintiffs' debit cards had not been among those compromised when P.F. Chang's experienced a security breach. Again, because P.F. Chang's initially announced that the breach affected all of its restaurants, the court found that the plaintiffs plausibly alleged a concrete harm caused by the defendant.[116]

The court declined to decide whether other alleged injuries were sufficient to establish standing. Among other things, plaintiffs alleged that they were injured by having to pay for their meals because they would not have dined at P.F. Chang's had they known its poor data security, which Judge Wood noted was an argument typically only accepted by

---

[113]*Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963, 967 (7th Cir. 2016).

[114]*See Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963, 967-68 (7th Cir. 2016).

[115]*See Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963, 967-68 (7th Cir. 2016).

[116]*See Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963, 968 (7th Cir. 2016).

courts in evaluating products that themselves were defective or dangerous, which consumers claim they would not have bought.[117] Plaintiffs also alleged a property right to their personally identifiable information.[118]

In applying *Remijas,* the court set a low bar for standing in *Lewert*, but one that ultimately was consistent with pre-*Clapper* Seventh Circuit law.

Thereafter, in *Dieffenbach v. Barnes & Noble, Inc*.,[119] the Seventh Circuit vacated a lower court ruling dismissing plaintiffs' complaint for failure to allege damage, holding that if a plaintiff establishes standing he or she establishes damage as well for purposes of stating a claim. Judge Easterbook, writing for himself, Chief Judge Wood and Circuit Judge Hamilton, in a brief opinion, characterized the lower court's ruling as involving "a new label for an old error."[120] He explained:

> To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available (if Barnes & Noble violated the statutes on which the claims rest). The plaintiffs have standing because the data theft may have led them to pay money for credit-monitoring services, because unauthorized withdrawals from their accounts cause a loss (the time value of money) even when banks later restore the principal, and because the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective. These injuries can justify money damages, just as they support standing.[121]

Judge Easterbrook then explained that plaintiffs had standing, and had alleged injury, under California and Illinois law, in a suit involving a security breach arising out of compromised PIN pads used to verify credit card information, where one plaintiff was injured because (1) her bank took three days to restore funds someone else had used to make a fraudulent purchase, (2) she had to spend time sort-

---

[117]*Lewert v. P.F. Chang's China Bistro Inc*., 819 F.3d 963, 968 (7th Cir. 2016).

[118]*See Lewert v. P.F. Chang's China Bistro Inc*., 819 F.3d 963, 968 (7th Cir. 2016).

[119]*Dieffenbach v. Barnes & Noble, Inc.,* 887 F.3d 826, 827-30 (7th Cir. 2018).

[120]*Dieffenbach v. Barnes & Noble, Inc.,* 887 F.3d 826, 828 (7th Cir. 2018).

[121]*Dieffenbach v. Barnes & Noble, Inc.,* 887 F.3d 826, 828 (7th Cir. 2018).

ing things out with the police and her bank, and (3) she could not make purchases using her compromised account for three days; and the other plaintiff alleged that (1) her bank contacted her about a potentially fraudulent charge on her credit card statement and deactivated her card for several days, and (2) the security breach at Barnes & Noble "was a decisive factor" when she renewed a credit-monitoring service for $16.99 per month.

At the same time the court cautioned that merely establishing standing did not mean the plaintiff could prevail.[122]

In an earlier case, *In re Target Corp. Data Security Breach Litigation*,[123] Judge Paul A. Magnuson of the District of Minnesota found standing in a case that at that time represented one of the largest data security breaches in U.S. history. Judge Magnuson held that plaintiffs who alleged that they incurred unlawful charges or faced restricted or blocked access to their bank accounts, along with an inability to pay other bills and charges for late payments or new cards, had standing to sue. He also ruled that some of the plaintiffs stated claims under various state consumer protection laws by alleging that Target (1) failed to maintain adequate computer systems and data security practices, (2) failed to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect consumers' personal and financial information, (3) failed to provide timely and adequate notice to plaintiffs of the breach,

---

[122]Judge Easterbrook explained:

> Everything we have said about California and Illinois law concerns injury. We have not considered whether Barnes & Noble violated any of these three state laws by failing to prevent villains from stealing plaintiffs' names and account data. Barnes & Noble was itself a victim. Its reputation took a hit, it had to replace the compromised equipment plus other terminals that had been shown to be vulnerable, and it lost business. None of the state laws expressly makes merchants liable for failure to crime-proof their point-of-sale systems. Plaintiffs may have a difficult task showing an entitlement to collect damages from a fellow victim of the data thieves. It is also far from clear that this suit should be certified as a class action; both the state laws and the potential damages are disparate. These and other questions need consideration on remand. That the case has been pending for 5½ years without a decision by the district court whether the proposed class can be certified is problematic under Fed. R. Civ. P. 23(c)(1)(A), which requires the decision to be made "[a]t an early practicable time after a person sues . . . as a class representative". All we hold today is that the complaint cannot be dismissed on the ground that the plaintiffs do not adequately allege compensable damages.

Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 830 (7th Cir. 2018).

[123]*In re Target Corp. Data Security Breach Litigation*, 66 F. Supp. 3d 1154 (D. Minn. 2014).

and (4) continued to accept plaintiffs' credit and debit cards for payments after Target knew or should have known of the data breach, but before it purged its systems of the hackers' malware. The court also allowed some plaintiffs to proceed to seek remedies available under state security breach notification laws,[124] to the extent available, while dismissing negligence claims under the laws of a number of states based on the economic loss rule. Judge Magnuson rejected plaintiffs' theory of unjust enrichment premised on the argument that every price of goods or services offered by Target included a premium for adequate security, to which class members were entitled. He did allow plaintiffs to proceed, however, with their claim for unjust enrichment premised on the theory that they would not have shopped at Target had they known the true state of Target's readiness for a potential security breach. The Target suit ultimately settled.[125]

As an example of the more typical analysis undertaken following *Clapper,* but before *Spokeo*, in *In re SAIC Corp*.,[126] the U.S. District Court for the District of Columbia held that the risk of identity theft alone and invasion of privacy to be insufficient to constitute "injury in fact," and the allegation that plaintiffs lost personal medical information to be too speculative in a security breach involving 4.7 million members of the U.S. military and their families. The court held that mere allegations that unauthorized charges were made to plaintiffs' credit and debit cards following the theft of data failed to show causation, but allegations that a specific plaintiff received letters in the mail from a credit card company thanking him for applying for a loan were sufficient. Similarly, the court held that the allegation that a plaintiff received a number of unsolicited calls from telemarketers and scam artists following the data breach did not suffice to show causation, but the allegation that unsolicited

---

[124]*See infra* § 27.08 (analyzing state security breach notification laws and remedies afforded for private causes of action, if any).

[125]*See In re Target Corp. Customer Data Security Breach Litigation*, 309 F.R.D. 482 (D. Minn. 2015) (providing preliminary approval of a class action settlement); *see also In re Target Corp. Customer Data Security Breach Litigation*, MDL No. 14-2522, 2015 WL 7253765 (D. Minn. Nov. 17, 2015) (granting final approval), *rev'd*, 847 F.3d 608 (8th Cir. 2017); *In re Target Corp. Customer Data Security Breach Litigation*, 892 F.3d 968 (8th Cir. 2018) (affirming final approval of a class action settlement, following remand).

[126]*In re SAIC Corp.*, 45 F. Supp. 3d 14 (D.D.C. 2014).

telephone calls were received on a plaintiff's unlisted number from insurance companies and others targeted at her specific, undisclosed medical condition were sufficient.[127]

In so ruling, Judge James E. Boasberg, Jr. held that the increased risk of harm alone does not confer standing; "as *Clapper* makes clear, . . . [t]he degree by which the risk of harm has increased is irrelevant – instead, the question is whether the harm is certainly impending."[128] He explained:

> Here, the relevant harm alleged is identity theft. A handful of Plaintiffs claim that they have suffered actual identity theft, and those Plaintiffs have clearly suffered an injury. At least twenty-four, however, allege only a risk of identity theft . . . . At this point, the likelihood that any individual Plaintiff will suffer harm remains entirely speculative. For identity theft to occur . . . the following chain of events would have to transpire: First, the thief would have to recognize the tapes for what they were, instead of merely a minor addition to the GPS and stereo haul. Data tapes, after all, are not something an average computer user often encounters. The reader, for example, may not even be aware that some companies still use tapes—as opposed to hard drives, servers, or even CDs—to back up their data . . . . Then, the criminal would have to find a tape reader and attach it to her computer. Next, she would need to acquire software to upload the data from the tapes onto a computer—otherwise, tapes have to be slowly spooled through like cassettes for data to be read . . . . After that, portions of the data that are encrypted would have to be deciphered. See Compl., ¶ 95 ("a portion of the PII/PHI on the data tapes was encrypted"). Once the data was fully unencrypted, the crook would need to acquire a familiarity with TRICARE's database format, which might require another round of special software. Finally, the larcenist would have to either misuse a particular Plaintiff's name and social security number (out of 4.7 million TRICARE customers) or sell that Plaintiff's data to a willing buyer who would then abuse it.[129]

Judge Boasberg acknowledged that his ruling was, "no doubt, cold comfort to the millions of servicemen and women who must wait and watch their credit reports until something untoward occurs. After all, it is reasonable to fear the worst in the wake of such a theft, and it is understandably frustrating to know that the safety of your most personal informa-

---

[127] *In re SAIC Corp.*, 45 F. Supp. 3d 14, 32–33 (D.D.C. 2014).

[128] *In re SAIC Corp.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014).

[129] *In re SAIC Corp.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014).

tion could be in danger."[130] He explained, however, that the Supreme Court "held that an 'objectively reasonable likelihood' of harm is not enough to create standing, even if it is enough to engender some anxiety . . . . Plaintiffs thus do not have standing based on risk alone, even if their fears are rational."[131]

Judge Boasberg noted that the Supreme Court in *Clapper* acknowledged "that it sometimes 'found standing based on a '*substantial risk*' that . . . harm will occur, which [could] prompt plaintiffs to reasonably incur costs to mitigate or avoid the harm.' "[132] In *SAIC,* however, the fact that breach victims had a 19% risk of experiencing identity theft meant that injury was likely not imminent for more than 80% of the victims (and the court suggested the actual number could be much higher "where the theft was unsophisticated and where the lack of widespread harm suggests that the tapes have not ever been accessed.").[133]

The Court in *SAIC* also distinguished pre-*Clapper* court opinions that allowed cases to move forward "where some sort of fraud had already taken place."[134] By contrast, *SAIC* involved "a low-tech, garden-variety" breach where two individuals alleged personalized injuries but there were no facts that "plausibly point[ed] to imminent, widespread harm" and where it remained likely that no one had accessed the personal information stored on the stolen tapes. Moreover, Judge Boasberg explained, the fact that two plaintiffs (Curtis and Yarde) could assert plausible claims does not lead to the conclusion that wide-scale disclosure and misuse of all 4.7 million TRICARE customers' data is plausibly

---

[130]*In re SAIC Corp.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014).

[131]*In re SAIC Corp.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014), *quoting Clapper*, 568 U.S. at 410-11.

[132]*In re SAIC Corp.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014), *quoting Clapper,* 568 U.S. at 414 n.5 (emphasis added by Judge Boasberg).

[133]*In re SAIC Corp.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014).

[134]*In re SAIC Corp.*, 45 F. Supp. 3d 14, 33 (D.D.C. 2014) (discussing *Anderson v. Hannaford Brothers*, 659 F.3d 151, 162–67 (1st Cir. 2011), where the First Circuit declined to question the plaintiffs' standing where 1,800 instances of credit- and debit-card fraud had already occurred and had been clearly linked to the data breach, and *Pisciotta v. Old National Bancorp.*, 499 F.3d 629, 632 (7th Cir. 2007), where "the court allowed plaintiffs to proceed where 'the scope and manner of access suggest[ed] that the intrusion was sophisticated, intentional and malicious,' and thus that the potential for harm was indeed substantial.").

"certainly impending."[135] After all, as previously noted,

> roughly 3.3% of Americans will experience identity theft of some form, regardless of the source . . . . So one would expect 3.3% of TRICARE's customers to experience some type of identity theft, even if the tapes were never read or misused. To quantify that percentage, of the 4.7 million customers whose data was on the tapes, one would expect around 155,100 of them to experience identity fraud simply by virtue of living in America and engaging in commerce, even if the tapes had not been lost. Here, only six Plaintiffs allege some form of identity theft, and out of those six only Curtis offers any plausible link to the tapes. And Yarde is the only other Plaintiff—out of a population of 4.7 million—who has offered any evidence that someone may have accessed her medical or personal information . . . . Given those numbers, it would be entirely implausible to assume that a massive identity–theft scheme is currently in progress or is certainly impending. Indeed, given that thirty-four months have elapsed, either the malefactors are extraordinarily patient or no mining of the tapes has occurred.[136]

Standing also proved elusive (or largely elusive) in a number of other security breach cases based on common law remedies, that were brought in various locations around the

---

[135] *Clapper*, 568 U.S. at 410.

[136] *In re SAIC Corp.*, 45 F. Supp. 3d 14, 34 (D.D.C. 2014). The Fourth Circuit subsequently cited this analysis with approval in *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017), in rejecting plaintiffs' statistical analysis as a basis for finding standing in a security breach case based on probabilities. In *Beck,* the Fourth Circuit explained that even if it were to credit plaintiffs' allegation that 33% of those affected by the data breaches would become victims of identity theft, "it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm." *Id., citing Khan v. Children's National Health System*, 188 F. Supp. 3d 524, 533 (D. Md. 2016) (holding that "general allegations . . . that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft" was insufficient to establish "substantial risk" of harm); *In re SAIC Corp.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (finding no "substantial risk" of harm where "[b]y Plaintiff's own calculations, then, injury is likely not impending for over 80% of victims").

The Fourth Circuit in *Beck* similarly rejected statistical evidence that data breach victims were 9.5 times more likely than the average person to suffer identity theft because "this general statistic says nothing about the risk arising out of any particular incident, nor does it address the particular facts of this case." *Beck v. McDonald*, 848 F.3d 262, 275 n.9 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

country following *Clapper* but before *Spokeo*.[137]

In *Spokeo, Inc. v. Robins*,[138] the U.S. Supreme Court considered the question of whether a plaintiff has Article III standing to sue for violation of a federal statute that does not require a showing of injury or harm if the plaintiff can state a claim under the statute but has not otherwise suffered any pecuniary loss. While most security breach cases are brought under common law theories such as breach of contract, breach of implied contract, breach of fiduciary duty or negligence, in a small percentage of cases, security breach claims may be brought under federal statutes.[139]

Prior to *Spokeo*, courts in the Sixth, Eighth and Ninth Circuits would find standing where a plaintiff could state a claim for violation of a statute, even if the statute does not require a showing of actual harm.[140] Courts in the Ninth Circuit had construed this rule, first articulated in *Edwards*

---

[137]*See, e.g.*, *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016) (dismissing plaintiff's tort, negligence, and statutory claims under Maryland law, arising out of a data security breach where plaintiffs alleged that defendants failed to secure adequately the computer hardware storing their customers' personal information, including their names, birth dates, email addresses, and subscriber identification numbers, for lack of Article III standing, because plaintiffs' alleged increased risk of future harm and current mitigation costs did not constitute injury-in-fact, nor did plaintiffs' alleged benefit of the bargain loss nor the alleged decreased value in their personal information), *appeal dismissed*, Appeal No. 16-1737 (4th Cir. Aug. 31, 2016); *Austin-Spearman v. AARP*, 119 F. Supp. 3d 1 (D.D.C. 2015) (holding that plaintiffs did not sustain an injury in fact resulting from their information having been shared where the defendant's privacy policy permitted the disclosure and, even if it had not, the plaintiff experienced no economic injury); *Green v. eBay, Inc.* , Civil No. 14–1688, 2015 WL 2066531 (E.D. La. May 4, 2015) (dismissing claim for lack of standing); *Storm v. Paytime, Inc.*, 90 F. Supp. 359 (M.D. Pa. 2015) (holding that employees lacked standing to sue over a cyber-attack, that incurring costs to take certain precautions following the breach was not an injury in fact, and that the attack was not an invasion of privacy); *Peters v. St. Joseph Services Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015) (holding that the increased risk of future identity theft or fraud was not a cognizable Article III injury and that even actual identity theft or fraud did not create standing where there was no injury). *But see Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 663-69 (E.D. Pa. 2015) (holding that the plaintiff had standing to pursue claims resulting from the theft or loss of a laptop containing his personal information).

[138]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[139]By comparison, data privacy cases frequently are brought under federal statutes. *See generally supra* § 26.15.

[140]*See Beaudry v. TeleCheck Services, Inc.*, 579 F.3d 702, 707 (6th Cir.

v. First American Corp.,[141] as requiring that even where a plaintiff states a claim under a federal statute that does not require a showing of damage, plaintiffs must allege facts to "show that the claimed statutory injury is particularized as to them."[142]

The Fourth and Federal Circuits, however, did not accept the proposition that alleging an injury-in-law by stating a claim and establishing statutory standing to sue satisfied the requirements for standing under Article III of the U.S. Constitution.[143]

When the U.S. Supreme Court granted certiorari in the

2009) (finding "no Article III (or prudential) standing problem arises . . ." where a plaintiff can allege all of the elements of a Fair Credit Reporting Act statutory claim); *Hammer v. Sam's East, Inc.*, 754 F.3d 492, 498–500 (8th Cir. 2014) (holding that plaintiffs established Article III standing by alleging facts sufficient to state a claim under the Fair and Accurate Credit Transactions Act (FACTA) and therefore did not separately need to show actual damage); *Robins v. Spokeo, Inc.*, 742 F.3d 409, 412–14 (9th Cir. 2014) (holding, in a case in which the plaintiff alleged that the defendant's website published inaccurate information about him, that because the plaintiff had stated a claim for a willful violation of the Fair Credit Reporting Act, for which actual harm need not be shown, the plaintiff had established Article III standing, where injury was premised on the alleged violation of plaintiff's statutory rights), *vacated and remanded*, 136 S. Ct. 1540 (2016); *Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), *cert. dismissed,* 567 U.S. 756 (2012); *supra* § 26.15.

[141]*Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), *cert. dismissed,* 567 U.S. 756 (2012).

[142]*Mendoza v. Microsoft, Inc.*, No. C14-316-MJP, 2014 WL 4540213 (W.D. Wash. Sept. 11, 2014) (dismissing plaintiffs' claims under the Video Privacy Protection Act, California Customer Records Act, California Unfair Competition Law and Texas Deceptive Trade Practices Act), *citing Jewel v. National Security Agency*, 673 F.3d 902, 908 (9th Cir. 2011); *see also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021 (N.D. Cal. 2012) (following *Edwards* and *Jewel* in finding standing in a data privacy case); *see generally supra* § 26.15.

[143]*See David v. Alphin*, 704 F.3d 321, 333, 338–39 (4th Cir. 2013) (holding that statutory standing alone is insufficient to confer Article III standing; affirming dismissal of an ERISA claim where the plaintiffs stated a claim but could not establish injury-in-fact); *Consumer Watchdog v. Wisconsin Alumni Research Foundation*, 753 F.3d 1258, 1262 (Fed. Cir. 2014) (holding that a consumer group lacked standing to challenge an administrative ruling, explaining that " 'Congress may enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute.' " *Linda R.S. v. Richard D.*, 410 U.S. 614, 617 n.3 (1973) (citations omitted). That principle, however, does not simply override the requirement of injury in fact.").

case then known as *Robins v. Spokeo, Inc.*,[144] many people assumed that the case, like *Clapper*, could present the Supreme Court with another opportunity for a 5-4 decision tightening the standards for establishing standing in federal court. Many observers predicted that the Court would conclude that Article III standing imposed an independent requirement for a plaintiff to show harm or injury to sue in federal court, even where the plaintiff could state a claim under a federal statute that itself did not require a showing of harm or injury to prevail. Instead, however, because Justice Scalia, a noted conservative jurist, passed away after oral argument but before a decision was rendered, the Court reached a compromise ruling in *Spokeo* that neither validated nor necessarily invalidated standing in cases involving only intangible harm.

In *Spokeo,* the Court held that merely alleging a "statutory violation" is *not* sufficient because "Article III standing requires a concrete injury even in the context of a statutory violation."[145] Justice Alito, writing for himself and five other justices, reiterated that to establish standing a plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision.[146] He further reiterated that the plaintiff bears this burden and, at the pleading stage, "must 'clearly . . . allege facts demonstrating' each element."[147] To establish an injury in fact, Justice Alito restated that a plaintiff must show that he or she has suffered " 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.' "[148]

For an injury to be *particularized,* it "must affect the

---

[144]*See Robins v. Spokeo, Inc.*, 742 F.3d 409, 412-14 (9th Cir. 2014), *cert. granted*, 135 S. Ct.1892 (2015).

[145]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[146]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.,* 528 U.S. 167, 180-81 (2000).

[147]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *quoting Warth v. Seldin,* 422 U.S. 490, 518 (1975).

[148]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992).

plaintiff in a personal and individual way."[149] Justice Alito explained that "[p]articularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be 'concrete.' "[150]

To be concrete, an injury must be " 'real' and not 'abstract.' "[151] It need not be *tangible,* however. "[I]ntangible injuries can . . . be concrete."[152]

In determining whether an intangible harm constitutes injury in fact, "both history and the judgment of Congress play important roles."[153] With respect to history, "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[154] For cases involving alleged statutory violations, Congress's "judgment is also instructive and important. . . . Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.' "[155]

While the Court made clear that merely alleging a "statutory violation" is not sufficient, Justice Alito also explained 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."[156] However, "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[157] For example, "a bare procedural violation, divorced from any concrete harm . . ."

---

[149]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 n.1 (1992).

[150]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016).

[151]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *citing* Webster's Third New Int'l Dictionary 472 (1971); Random House Dictionary of the English Language 305 (1967).

[152]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[153]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[154]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[155]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 578 (1992).

[156]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 580 (1992).

[157]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

would not satisfy the injury-in-fact requirement.[158] On the other hand, "the risk of real harm" can satisfy the requirement of concreteness and, in some circumstances, even "the violation of a procedural right granted by statute can be sufficient . . . ."[159]

In remanding the case for further consideration, Justice Alito reiterated that the plaintiff in that case could not satisfy the demands of Article III by alleging a bare procedural violation of the Fair Credit Reporting Act. Similarly, Justice Alito offered that if the defendant had maintained an incorrect zip code for the plaintiff, "[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[160]

Thus, under *Spokeo,* where an injury is only intangible, whether injury in fact exists, to establish one of the prongs of the test for standing, will depend on (1) the "historical practice" of English and American courts and (2) Congress's role in identifying and elevating to the status of legally cognizable concrete injuries, harms that otherwise would not be sufficient.

Justice Thomas concurred in the decision, drawing a distinction between private and public rights. Justices Ginsburg and Sotomayor dissented, arguing that the plaintiff established standing in this case.

Spokeo ultimately leaves unanswered questions about its scope. In security breach cases involving common law claims, it validates the notion that intangible harm may be sufficient to establish injury in fact, but does not alter the ruling in *Clapper* on when the threat of future harm will provide grounds for standing. For both common law and statutory claims, it requires that intangible harm be concrete and particularized and of the type traditionally recognized as actionable by English or American courts[161] or, for claims premised on federal statutes, one that Congress sought to

---

[158]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *citing Summers v. Earth Island Institute,* 555 U.S. 488, 496 (2009).

[159]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[160]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016). On remand, the Ninth Circuit concluded that Robins had standing under the Supreme Court's test. *See Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir. 2017).

[161]*See, e.g., Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 34 (2d Cir. 2017) (affirming the lower court ruling that the plaintiffs had adequately alleged standing to assert state law claims of deceptive business practices

elevate[162] to a concrete injury. For claims brought under

---

under N.Y. Gen. Bus. Law § 349 and unjust enrichment, based on loss of privacy, because PulsePoint's allegedly unauthorized accessing and monitoring of plaintiffs' web-browsing activity implicated "harms similar to those associated with the common law tort of intrusion upon seclusion so as to satisfy the requirement of concreteness.").

[162]*See, e.g., Strubel v. Comenity Bank*, 842 F.3d 181, 190-95 (2d Cir. 2016) (holding that the failure of a bank to notify the holder of a store-branded credit card of his rights and obligations regarding disputed credit card purchases in violation of the Truth in Lending Act was sufficient to confer Article III standing because the lack of notice could result in a consumer losing the ability to exercise rights under the Truth in Lending Act (TILA), but that the bank's failure to notify the holder of billing error corrections, pursuant to TILA, did not confer Article III standing because there was no "plausible claim of adverse effects on consumer behavior" by the failure to provide the notice); *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 629, 638–40 (3d Cir. 2017) (holding that plaintiffs had standing to sue for the disclosure of personal information, in violation of FCRA, as a result of the theft of two laptops, because "[i]n light of the congressional decision to create a remedy for the unauthorized transfer of personal information, a violation of FCRA gives rise to an injury sufficient for Article III standing purposes. Even without evidence that the Plaintiffs' information was in fact used improperly, the alleged disclosure of their personal information created a de facto injury."; holding that the injury was not merely procedural, but involved "unauthorized dissemination of their own private information—the very injury that FCRA is intended to prevent" and noting that "[w]e are not suggesting that Horizon's actions would give rise to a cause of action under common law . . . [but] since the 'intangible harm' that FCRA seeks to remedy 'has a close relationship to a harm [i.e., invasion of privacy] that has traditionally been regarded as providing a basis for a lawsuit in English or American courts,' *Spokeo*, 136 S. Ct. at 1549, . . . Congress properly defined an injury that 'give[s] rise to a case or controversy where none existed before.' "); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 272-74 (3d Cir. 2016) (holding, without much analysis, that plaintiffs had Article III standing to pursue Stored Communications Act, Video Privacy Protection Act, California Invasion of Privacy Act, New Jersey computer crime and common law privacy claims), *cert. denied,* 137 S. Ct. 624 (2017); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 982-84 (9th Cir. 2017) (affirming dismissal on the merits, but first holding that the plaintiff had standing to sue for the alleged disclosure of personally identifiable information under the Video Privacy Protection Act, which the Ninth Circuit panel deemed an alleged violation of "a substantive provision that protects concrete interest."); *Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037, 1042-43 (9th Cir. 2017) (holding that the plaintiff had alleged sufficient harm to establish Article III standing in a TCPA case because (1) "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts, and the right of privacy is recognized by most states" and (2) Congress, in enacting the statute, established "the substantive right to be free from certain types of phone calls and text messages absent consumer consent."); *Perry v. CNN*,

federal statutes, *Spokeo* suggests, at a minimum, that standing may be absent where an alleged violation is procedural in nature and the plaintiff suffers no harm (as appellate courts subsequently have held in cases involving the Fair and Accurate Credit Transactions Act (FACTA),[163] the Cable

---

854 F.3d 1336, 1339-41 (11th Cir. 2017) (holding that a user of the CNN mobile app had standing to sue under the Video Privacy Protection Act, where he alleged no injury other than the statutory violation, because (1) "[t]he structure and purpose of the VPPA supports the conclusion that it provides actionable rights" in prohibiting the wrongful disclosure of personal information, and (2) a VPPA claim has a close relationship to a common law right of privacy, which is a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts, where "[t]he intrusion itself makes the defendant subject to liability, even though there is no publication or other use . . ."; *citing* Restatement of Torts § 652B cmt. B); *Church v. Accretive Health, Inc.,* 654 F. App'x 990 (11th Cir. 2016) (finding standing under *Spokeo,* in an unreported decision, where the plaintiff failed to receive certain informational disclosures to which she was entitled under the Fair Debt Collection Practices Act).

[163]15 U.S.C. § 1681c(g)). FACTA seeks to reduce the risk of identity theft by, among other things, prohibiting merchants from including more than the last five digits of a customer's credit card number on a printed receipt. *See* 15 U.S.C. § 1681c(g)(1); *see generally supra* § 26.12[8]. Courts have found standing to be lacking in FACTA cases involving bare procedural violations. *See, e.g., Katz v. Donna Karan, LLC,* 872 F. 3d 114 (2d Cir. 2017) (affirming dismissal, for lack of standing, of plaintiff's FACTA claim alleging that he twice purchased items at the defendants' stores, and on both occasions received a printed receipt that identified not only the last four digits of his credit card number but also the first six digits, because plaintiff could not meet his affirmative burden to establish subject matter jurisdiction by a preponderance of the evidence); *Crupar–Weinmann v. Paris Baguette America, Inc*., 861 F.3d 76, 81 (2d Cir. 2017) (affirming the lower court's holding that a procedural violation of FACTA—the printing of the plaintiff's credit card expiration date on her receipt—presented no material risk of harm to the underlying interest Congress sought to protect (identity theft), because Congress itself had clarified that printing the expiration date, without more, did not "increase . . . the risk of material harm of identity theft."); *Meyers v. Nicolet Restaurant of De Pere, LLC,* 843 F.3d 724, 726-29 (7th Cir. 2016) (holding that plaintiff lacked standing to sue for a FACTA violation alleging that the defendant failed to provide him with a receipt that truncated the expiration date of his credit card because "without a showing of injury apart from the statutory violation, the failure to truncate a credit card's expiration date is insufficient to confer Article III standing."); *Bassett v. ABM Parking Services, Inc.*, 883 F.3d 776, 779-83 (9th Cir. 2018) (holding that receiving "an overly revealing credit card receipt—unseen by others and unused by identity thieves . . ." constituted a procedural violation of the FCRA that was insufficient to establish Article III standing; "We need not answer whether a tree falling in the forest makes a sound when no one is there to hear it. But when this receipt fell into Bassett's hands in a parking garage

Communications Privacy Act,[164] other privacy statutes,[165]

---

and no identity thief was there to snatch it, it did not make an injury."); *see also Daniel v. National Park Service*, 891 F.3d 762, 766-68 (9th Cir. 2018) (distinguishing *Bassett* in finding that the plaintiff had alleged a concrete, particularized injury based on identity theft and fraudulent charges that occurred after she received a debit card receipt at Yellowstone National Park that displayed the expiration date of her credit card, but holding that Article III standing was lacking because she had not alleged an injury "fairly traceable" to the violation because her actual debit card number was partially obscured and there were no facts to suggest that the exposure of the expiration date resulted in the identity theft or fraudulent charges).

[164]*See, e.g.*, *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 910-12 (7th Cir. 2017) (holding that the plaintiff lacked standing to sue for Time Warner's alleged retention of his personally identifiable information in violation of the Cable Communications Policy Act, 47 U.S.C. § 551(e), because he did not allege that "any of the personal information that he supplied to the company . . . had been leaked or caused financial or other injury to him or had even been at risk of being leaked."; Although the Act created a right of privacy, and "[v]iolations of rights of privacy are actionable," because plaintiff did not allege that "Time Warner had released, or allowed anyone to disseminate, any of the plaintiff's personal information in the company's possession," the statutory violation alone could not confer standing); *Braitberg v. Charter Communications, Inc.,* 836 F.3d 925, 929-31 (8th Cir. 2016) (dismissing for lack of standing, as a case involving a mere procedural violation under *Spokeo,* plaintiff's putative class action suit alleging that his former cable television provider retained his personally identifiable information in violation of the Cable Communications Policy Act because "Braitberg alleges only that Charter violated a duty to destroy personally identifiable information by retaining certain information longer than the company should have kept it. He does not allege that Charter has disclosed the information to a third party, that any outside party has accessed the data, or that Charter has used the information in any way during the disputed period. He identifies no material risk of harm from the retention; a speculative or hypothetical risk is insufficient. Although there is a common law tradition of lawsuits for invasion of privacy, the retention of information lawfully obtained, without further disclosure, traditionally has not provided the basis for a lawsuit in American courts.").

[165]*See, e.g.*, *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12, 15-17 (2d Cir. 2017) (holding that players of Take-Two's NBA 2K15 video game, which scanned players' faces, did not have Article III standing to sue for alleged violations of the Illinois Biometric Information Privacy Act, which was intended to protect against potential misuse of biometric data, because plaintiffs' alleged failure to comply with provisions regulating the storage and dissemination of biometric information and requiring notice and consent to the collection of biometric information amounted to merely "procedural violations" under *Spokeo*, where no reasonable player would have concluded that the MyPlayer feature was conducting anything other than a face scan where plaintiffs had to place

and other federal[166] and state laws[167]). *Spokeo*'s impact on

---

their faces within 6-12 inches of the camera, slowly turn their heads to the left and right, and continue to do this for approximately 15 minutes, belying any claim of lack of consent; plaintiffs could not allege any material risk of misuse of biometric data for failing to provide notice of the duration for which the data would be held; and plaintiffs failed to show a risk of real harm from the alleged unencrypted transmission of their face scans); *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (affirming dismissal of plaintiff's claim under the D.C.'s Use of Consumer Identification Information Act, D.C. Code §§ 47–3151 *et seq*., which provides that "no person shall, as a condition of accepting a credit card as payment for a sale of goods or services, request or record the address or telephone number of a credit card holder on the credit card transaction form, . . ." for lack of standing, because "[t]he Supreme Court's decision in *Spokeo* . . . closes the door on Hancock and White's claim that the Stores' mere request for a zip code, standing alone, amounted to an Article III injury."); *see also In re U.S. Office of Personnel Management Data Security Breach Litig.*, 266 F. Supp. 3d 1, 19–26 (D.D.C. 2017) (holding that Federal employees did not have standing to sue over a cybersecurity breach by a contractor of the U.S. Office of Personnel Management, noting that "Congress carefully limited the remedies that would be available in a Privacy Act case, and it specifically added the requirement of a showing of actual harm beyond the statutory violation and its impact on one's privacy before the government would be required to answer in Court.").

[166]*See, e.g.*, *Lee v. Verizon Communications, Inc.*, 837 F.3d 523, 529–30 (5th Cir. 2016) (holding that plaintiff had no standing where the plaintiff alleged breach of a duty under ERISA but no harm caused by the alleged mismanagement of a pension plan); *Hagy v. Demers & Adams*, 882 F.3d 616 (6th Cir. 2018) (holding that mortgagors lacked Article III standing for their Fair Debt Collection Practices Act ("FDCPA") claim); *Lyshe v. Levy*, 854 F.3d 855 (6th Cir. 2017) (affirming dismissal of plaintiffs' FDCPA claim based on appellees' alleged violation of state procedural rules requiring that discovery responses to requests for admission be sworn and notarized); *Academy of Doctors of Audiology v. Int'l Hearing Society*, 237 F. Supp. 3d 644, 650-60 (E.D. Mich. 2017) (dismissing plaintiff's Lanham Act false advertising claim for lack of Article III standing); *Cohen v. Facebook Inc.*, 252 F. Supp. 3d 140, 149-50 (E.D.N.Y. 2017) (dismissing the claims brought by current Israeli citizens who feared terrorist attacks allegedly due to Hamas's use of Facebook, for lack of Article III standing to assert claims under the Anti-Terrorism Act, 18 U.S.C.A. § 2333(a), the Justice Against Sponsors of Terror Acts, 18 U.S.C.A. § 2333, and provision of material support to terrorist groups in violation of 18 U.S.C.A. §§ 2339A and 2339B).

[167]*See, e.g., Ross v. AXA Eq. Life Ins. Co.*, 680 F. App'x 41, 45-46 (2d Cir. 2017) (affirming dismissal of plaintiffs' claims under New York law, where they argued that they had suffered an injury in fact based on an increased risk that their insurer would be unable to pay future claims due to alleged misrepresentations, which the court deemed "too far down the speculative chain of possibilities to be 'clearly impending' "); *Nicklaw v.*

putative data privacy and TCPA class action suits is addressed in sections 26.15 and 29.16, respectively.

Citimortgage, Inc., 839 F.3d 998, 1002–03 (11th Cir. 2016) (holding that plaintiff had no standing to sue under a New York state statute where he alleged that the defendant failed to record a satisfaction of a mortgage within the required 30 days under a state statute but alleged no harm flowing from that failure); *Antman v. Uber Technologies, Inc.*, Case No. 3:15-cv-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018) (dismissing, with prejudice, plaintiff's claims, arising out of a security breach, for allegedly (1) failing to implement and maintain reasonable security procedures to protect Uber drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract, for lack of Article III standing, where plaintiff could not allege injury sufficient to establish Article III standing); *Murray v. Lifetime Brands, Inc.,* Civil Action No. 16–5016, 2017 WL 1837855 (D.N.J. May 8, 2017) (dismissing plaintiff's suit, which alleged that the defendant's Terms of Service violated the New Jersey Truth-in-Consumer Contract, Warranty and Notice Act, for lack of Article III standing); *Rubin v. J. Crew Group, Inc.,* Civil Action No. 16-2167 (FLW), 2017 WL 1170854 (D.N.J. Mar. 29, 2017) (dismissing plaintiff's claim that J. Crew's online Terms of Service violated the TCCWNA for lack of Article III standing, admonishing that "[w]hile the intent of the New Jersey legislature in enacting the TCCWNA is to provide additional protections for consumers in this state from unfair business practices, the passage of the Act is not intended . . . for litigation-seeking plaintiffs and/or their counsel to troll the internet to find potential violations under the TCCWNA without any underlying harm."); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, Case No.: 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *2-9 (S.D. Cal. Nov. 3, 2016) (dismissing plaintiff's section 1798.82 and most of his 1798.81.5 claims for lack of Article III standing based on the risk of future identity theft (except for § 1798.81.5, UCL, right of privacy, and negligence claims based on lost time), in a suit alleging that the defendant had failed to maintain reasonable security "because the PII stolen was limited only to Plaintiff's name, address, and credit card information, and because the credit card has since been cancelled," and where the plaintiff had not "specifically alleged out-of-pocket losses or monetary damages resulting from the data breach due to Defendants' negligence or "failure to maintain reasonable security procedures." *See generally* Cal. Civ. Code § 1798.81.5(b)."); *Castillo v. Seagate Technology, LLC*, Case No. 16-cv-01958-RS, 2016 WL 9280242, at *7 (N.D. Cal. Sept. 14, 2016) (denying defendant's motion to dismiss plaintiff's section 1798.80 and 1798.81.5 claims, arising out of a security breach, while dismissing other claims with leave to amend).

The TCCWNA is separately analyzed in section 22.05[2][R], where a larger number of cases addressing standing under that statute are addressed.

California state data security laws are addressed in section 27.04[6][C].

Following *Spokeo,* the Sixth Circuit, in *Galaria v. Nationwide Mutual Insurance Co.*,[168] an unreported 2-1 decision, reversed and remanded the lower court's holding that the plaintiff could not establish standing to assert a Fair Credit Reporting Act claim in a security breach case. Relying on *Remijas* and *Lewert,* the majority held that the plaintiffs alleged a substantial risk of harm coupled with reasonably incurred mitigation costs where they alleged that data submitted for insurance quotes (which included a person's name, birth date, marital status, gender, occupation, employer, Social Security number and driver's license number) had been stolen and was now in the hands of ill-intentioned criminals. Unlike the data at issue in *Lewert,* this was the type of data that could have allowed for identity theft, although none had occurred in this case.

As in *Remijas,* the majority in *Galaria* cited Nationwide's willingness to provide credit monitoring and identity theft protection for a year as evidence that Nationwide itself recognized the severity of the threat. Judge Helen N. White, writing for herself and Western District of Tennessee District Judge Sheryl H. Lipman (who was sitting by designation), explained that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaint." Although the court conceded that it was not "literally certain" that plaintiffs' data would be misused, there was "a sufficiently substantial risk of harm that incurring mitigation costs is reasonable. Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security, particularly when Nationwide recommended taking these steps."

Although Nationwide had provided a year of credit monitoring services, plaintiffs alleged that they needed to spend time and money to monitor their credit, check their bank statements, and modify their financial accounts. They also alleged that they incurred costs to obtain credit freezes that

[168] *Galaria v. Nationwide Mutual Insurance Co.,* 663 F. App'x 384 (6th Cir. 2016).

Nationwide recommended but did not cover.[169] Accordingly, the majority found that this was "not a case where Plaintiffs seek to 'manufacture standing by incurring costs in anticipation of non-imminent harm.' . . . Rather, these costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing."

Although the majority in *Galaria* referred to *costs,* in all likelihood what plaintiffs incurred was the inconvenience of spending time monitoring and changing their accounts and requesting a credit freeze and did not incur any hard costs unless they hired a third party to help them. It does not appear, however, that the majority in this unreported decision appreciated this point in taking at face value the allegation of lost costs. What this case in fact involved was inconvenience and lost time or the threat of future harm.[170]

Addressing the second and third factors identified in *Spokeo,* the majority found the alleged harm traceable to Nationwide because for purposes of standing, only general causation, not proximate cause, must be shown. It also found that plaintiffs' harm could be redressed by a favorable ruling in the case.

In finding standing, Judge White distinguished *Reilly v. Ceridian Corp.*[171] as a case where there was no evidence that the intrusion was intentional or malicious. In fact, however, the Third Circuit's ruling in *Reilly* takes a different approach to standing in security breach cases, which is more skeptical of intangible harm where there has been no actual identity

---

[169]A credit freeze can only be requested by a consumer. Since 2018, there has been no charge associated with placing a credit freeze on an account and obtaining a year of fraud alerts, unless a consumer hires a third party to help them with the request.

[170]In a confusing footnote, the majority, in *dicta,* notes that plaintiff Galaria also alleged that he suffered three unauthorized attempts to open credit cards in his name, which further supported standing, although this allegation appears only in a proposed amended Complaint addressing only the Fair Credit Reporting Act claim and appears to have been waived with respect to plaintiffs' negligence and bailment claims. *See id.* n.1. Although not discussed in the unreported Sixth Circuit opinion, plaintiffs had alleged below that they were 9.5 times more likely than members of the general public to be victims of identity theft, as a result of this breach, reflecting a fraud incidence rate of 19%. *See Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 654 (S.D. Ohio 2014), *rev'd*, 663 F. App'x 384 (6th Cir. 2016).

[171]*Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied,* 566 U.S. 989 (2012).

theft.

Judge Alice M. Batchelder dissented, arguing that the court did not need to "take sides in the existing circuit split regarding whether an increased risk of identity theft is an Article III injury" because, whether or not it was, the plaintiffs had "failed to demonstrate the second prong of Article III standing—causation." Judge Batchelder argued that this case was distinguishable from other security breach cases, including the Sixth Circuit's own previous decision in *Lambert v. Hartman*,[172] because *Galaria* involved an intervening criminal act by a third party hacker, where the plaintiffs failed to allege any factual causal link between their alleged injury—an increased risk of identity theft—and "something Nationwide did or did not do." In writing that she would have affirmed the lower court's order finding no standing, Judge Batchelder criticized the Seventh Circuit's opinions in *Remijas* and *Lewert* and the Eleventh Circuit's earlier opinion in *Resnick v. AvMed, Inc.*,[173] as decisions that "completely ignore[d] the independent third party criminal action breaking the chain of causation."

In *Attias v. Carefirst, Inc.*,[174] the D.C. Circuit also followed Seventh Circuit law on standing in breach cases where there has been no identity theft, in holding that plaintiffs plausibly alleged a heightened risk of future injury from defendant's data security breach that was substantial enough to justify Article III standing. In that case, plaintiffs asserted that a cyberattack on Carefist allowed an intruder to gain access to plaintiffs' personal information, including their names, birth dates, email addresses, subscriber ID numbers, credit card information and social security numbers, placing plaintiffs at high risk of identity theft. Two of the plaintiffs actually alleged that they had been the victims of identity theft, but the court did not separately consider these allegations because of its conclusion that all of the plaintiffs had stand-

---

[172]*See Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008) (finding standing to bring a constitutional right to privacy claim where plaintiff's information was posted on a municipal website and then taken by an identity thief, causing her actual financial loss fairly traceable to the defendant's conduct), *cert. denied*, 555 U.S. 1126 (2009).

[173]*Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012).

[174]*Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

ing to sue based on their heightened risk of identity theft.[175]

The D.C. Circuit followed the Seventh Circuit's decision in *Remijas v. Neiman Marcus Group, LLC*,[176] in concluding that it was plausible to infer that a party accessing plaintiffs' personal information did so with "both the intent and ability to use the data for ill."[177] Judge Thomas B. Griffin, writing for the panel which also included Circuit Judges Patricia Ann Millett and David S. Tatel, elaborated that "[a]s the Seventh Circuit asked, in another data breach case where the court found standing, 'Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.' "[178] The court also noted that plaintiffs' names, birth dates, email addresses and subscriber identification numbers alone could allow for " 'medical identity theft' in which a fraudster impersonates the victim and obtains medical services in her name."[179] Under *Attias,* standing in D.C. courts may be established in a security breach case involving the risk of future harm by showing *either* that future harm is "certainly impending" *or* that there is a "substantial risk that the harm will occur."[180]

Although *Attias* was decided in August 2017, the court did not reference potentially conflicting circuit court decisions from other circuits that had been decided earlier in 2017, which take a different approach from the Seventh Circuit—namely, *Whalen v. Michaels Stores, Inc.*[181] and *Beck v.*

---

[175]*See Attias v. Carefirst, Inc.*, 865 F.3d 620, 626 n.2 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[176]*Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

[177]*Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[178]*Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017) (*quoting Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015)), *cert. denied*, 138 S. Ct. 981 (2018).

[179]*Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[180]*Attias v. Carefirst, Inc.*, 865 F.3d 620, 626-27 (D.C. Cir. 2017) (quoting *Susan B. Anthony List v. Diehaus*, 134 S. Ct. 2334, 2341 (2014)), *cert. denied*, 138 S. Ct. 981 (2018).

[181]*Whalen v. Michaels Stores, Inc.,* 689 F. App'x 89 (2d Cir. 2017).

McDonald.[182]

In *Whalen v. Michaels Stores, Inc.*,[183] a non-precedential opinion from the Second Circuit, an appellate panel comprised of Judges Guido Calabresi, Susan L. Carney and Eastern District of New York Judge Carol Bagley Amon, sitting by designation, affirmed the lower court ruling that the plaintiff lacked standing to sue for breach of implied contract and under N.Y. Gen. Bus. L. § 349. Plaintiff alleged that she made purchases via a credit card at a Michaels store on December 31, 2013, and that Michaels experienced a breach that exposed credit card numbers but no other information such as a person's name, address or PIN. Plaintiff further alleged that her credit card was presented for unauthorized charges in Ecuador on January 14 and 15, 2014, that she faced a risk of future identity fraud and that she had lost time and money resolving the attempted fraudulent charges and monitoring her credit, but the court held that this was insufficient to establish standing where she did not allege that any fraudulent charges were actually incurred by her prior to the time she canceled her card on January 15 or that, before the cancellation, she was in any way liable on account of those presentations, and where she did not allege with any specificity that she spent time or money monitoring her credit. The court explained that:

> Whalen does not allege a particularized and concrete injury suffered from the attempted fraudulent purchases, however; she never was either asked to pay, nor did pay, any fraudulent charge. And she does not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen. Finally, Whalen pleaded no specifics about any time or effort that she herself has spent monitoring her credit."[184]

In *Beck v. McDonald*,[185] the Fourth Circuit held that patients at a Veterans Affairs hospital who sued under the

---

[182]*Beck v. McDonald*, 848 F.3d 262 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

[183]*Whalen v. Michaels Stores, Inc.,* 689 F. App'x 89 (2d Cir. 2017).

[184]*Whalen v. Michaels Stores, Inc.,* 689 F. App'x 89, 90-91 (2d Cir. 2017).

[185]*Beck v. McDonald*, 848 F.3d 262 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

Privacy Act[186] and Administrative Procedure Act[187] alleging that their personal information had been compromised as a result of two data breaches did not have standing because (a) an enhanced risk of future identity theft was too speculative to cause injury-in-fact and (b) the allegations were insufficient to establish a substantial risk of harm.[188] The court also rejected the argument that the cost of mitigation measures provided grounds for standing.[189]

Beck involved two separate cases –in one, the district court had granted summary judgment for the defendant (*Beck*), based on evidence presented, while in the other one (*Watson*), the court had granted defendant's motion to dismiss.

In *Beck*, a laptop connected to a pulmonary function testing device containing the unencrypted personal information of 7,400 patients—including their names, birth dates, the last four digits of their social security numbers, and physical descriptors (age, race, gender, height, and weight)—was stolen or misplaced. Plaintiffs had sued alleging that based on statistical evidence, 33% of those affected would have their identities stolen and that all those affected would be 9.5 times more likely to experience identity theft. They also alleged a present injury because they purchased credit monitoring series and took other steps to mitigate what the district court had characterized as "the speculative future harm of identity theft."[190]

In the companion *Watson* case, identifying information of over 2,000 patients—including their names, social security numbers and medical diagnoses—had been placed in four boxes of pathology reports that had been lost or stolen en route to long term storage. The district court ruled that plaintiff's alleged risk of future harm based on these facts was dependent on an "attenuated chain of possibilities" that did not satisfy Watson's burden to show that her threatened

---

[186]5 U.S.C. §§ 552a *et seq*.

[187]5 U.S.C. §§ 701 *et seq*.

[188]*See Beck v. McDonald*, 848 F.3d 262, 269-76 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

[189]*See Beck v. McDonald*, 848 F.3d 262, 276-77 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

[190]*Beck v. McDonald*, 848 F.3d 262, 268 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

injury was "certainly impending."[191] For the same reason as in *Beck*, the district court rejected Watson's argument that it had shown injury-in-fact because she had incurred costs to fend off future identity theft.

In affirming no injury-in-fact in either case, Judge Albert Diaz—writing for the Fourth Circuit panel which also included Circuit Judge Paul Niemeyer and West Virginia District Court Judges Irene M. Keeley (who was sitting by designation)—reiterated that to establish standing, "a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.' "[192] Quoting the Supreme Court, the Fourth Circuit reiterated that "[a]lthough 'imminence' is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes."[193] Applying the Supreme Court's holding in *Clapper,* the court found no standing based either on the enhanced risk of future identify theft or the mitigation costs associated with protecting against this risk.

With respect to the alleged enhanced risk of future identity theft, the Fourth Circuit held that "the mere theft" of information, "without more, cannot confer Article III standing."[194] The appellate panel distinguished cases applying the more

---

[191]*Beck v. McDonald*, 848 F.3d 262, 269 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017). The court explained that for Watson to suffer the injury she feared, the court would have to assume that:

> (1) the boxes were stolen by someone bent on misusing the personal information in the pathology reports; (2) the thief would select Watson's report from the over 3,600 reports in the missing boxes; (3) the thief would then attempt to use or sell to others Watson's personal information; and (4) the thief or purchaser of Watson's information would successfully use the information in the report to steal Watson's identity.

Id.

[192]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *quoting* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

[193]*Beck v. McDonald*, 848 F.3d 262, 271 (4th Cir.) (*quoting Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564-65 n.2 (1992)), *cert denied,* 137 S. Ct. 2307 (2017).

[194]*Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir.) (*citing Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007) (deeming as speculative plaintiffs' allegations "that at some unspecified point in the indefinite future they will be the victims of identity theft" where, although plaintiffs clearly alleged their information was stolen by a burglar, they did "not allege that the burglar who stole the laptop did so in order

liberal Seventh Circuit test because those cases involved a data thief intentionally targeting personal information that was compromised in a breach.[195] The court also differentiated cases where at least one named plaintiff alleged misuse or access by the thief.[196] By contrast, in the two consolidated cases in *Beck,* the Fourth Circuit emphasized that the breaches had occurred in February 2013 and July 2014 and, even after extensive discovery in one of the cases, plaintiffs had found "no evidence that the information contained on the stolen laptop" had been "accessed or misused or that they ha[d] suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information."[197] The court explained that " 'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative."[198] To assume that plaintiffs would in fact suffer identity theft, the court explained, would require engaging "in the same 'attenuated chain of possibilities' rejected by the [Supreme] Court in

---

to access their [i]nformation, or that their [i]nformation ha[d] actually been accessed since the laptop was stolen")), *cert denied,* 137 S. Ct. 2307 (2017).

[195]*Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir.) (citing *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692, 694 (7th Cir. 2015); *Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384, 387-89 (6th Cir. 2016); and *Pisciotta v. Old National Bancorp.*, 499 F.3d 629, 632 (7th Cir. 2007)), *cert denied,* 137 S. Ct. 2307 (2017).

[196]*Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir.) (citing *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 690 (7th Cir. 2015) (where 9,200 of the 350,000 credit cards potentially exposed to malware "were known to have been used fraudulently"); and *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010) (where the plaintiff alleged that, two months after the theft of a laptop containing his social security number, someone attempted to open a new account using his social security number)), *cert denied,* 137 S. Ct. 2307 (2017).

[197]*Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

[198]*Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir.) (*citing Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016); *In re Zappos.com*, 108 F. Supp. 3d 949, 958 (D. Nev. 2015) ("[T]he passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something.")), *cert denied,* 137 S. Ct. 2307 (2017). *But see In re Zappos.com, Inc.*, 888 F.3d 1020, 1028-29 & n.13 (9th Cir. 2018) (discussing *Beck* but crediting the allegations in plaintiffs' Complaint that a person whose PII has been obtained and compromised may not see the full extent of identity theft or identity fraud for years and it may take some time for the victim to become aware of the theft).

Clapper."[199] Accordingly, the appellate panel agreed with the district court that plaintiffs failed to meet their respective burdens to either "plausibly plead" factual allegations or "set forth particular evidence" sufficient to show that the threatened harm of future identity theft was "certainly impending."

The appellate panel also rejected plaintiffs' argument that it suffered "adverse effects" sufficient to establish standing based on "emotional upset" and fear of identity theft and fraud resulting from the data breaches.[200]

The court further rejected standing based on the increased risk of future identity theft by analogy to environmental standing cases to support their view that only a "reasonable concern" of harm should be sufficient to confer Article III standing. The appellate court explained, however that in environmental litigation, the standing requirements are less onerous because "[t]he extinction of a species, the destruction of a wilderness habitat, or the fouling of air and water are harms that are frequently difficult or impossible to remedy" by monetary compensation. . . . By contrast, in data-breach cases, 'there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely.' "[201]

The Fourth Circuit panel also affirmed the lower court's finding of no standing based on a "substantial risk" that harm will occur, which in turn may cause a party to reason-

---

[199]*Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir.) (*quoting Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410, 414 n.5 (2013)), *cert denied,* 137 S. Ct. 2307 (2017). The court explained that:

> In both cases, we must assume that the thief targeted the stolen items for the personal information they contained. And in both cases, 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. This "attenuated chain" cannot confer standing.

848 F.3d at 275.

[200]*Beck v. McDonald*, 848 F.3d 262, 272 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017). The court characterized this argument as reflecting "a misunderstanding of the Privacy Act" and representing "an overextension of *Doe v. Chao*, 540 U.S. 614 (2004)." 848 F.3d at 272.

[201]*Beck v. McDonald*, 848 F.3d 262, 274 n.5 (4th Cir.) (first case quotation omitted) (*quoting Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied*, 566 U.S. 989 (2012)), *cert denied,* 137 S. Ct. 2307 (2017).

ably incur costs to mitigate or avoid that harm.[202] In addressing plaintiffs' statistical evidence, the court wrote that even if the court credited the plaintiffs' allegation that 33% of those affected by the data breaches would become victims of identity theft, "it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm."[203] It likewise rejected statistical evidence that data breach victims were 9.5 times more likely than the average person to suffer identity theft because "this general statistic says nothing about the risk arising out of any particular incident, nor does it address the particular facts of this case."[204]

The Fourth Circuit likewise rejected plaintiffs' argument that because defendants offered credit monitoring services, this evidenced a substantial risk of harm. In so ruling, the Fourth Circuit declined to follow the Seventh Circuit rule (which was also applied in a non-precedential Sixth Circuit case).[205] The Fourth Circuit explained that:

> 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. To adopt such a presumption would surely discourage organizations from offering these services to data-

---

[202] *Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir.) (*citing Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 414 n.5 (2013)), *cert denied,* 137 S. Ct. 2307 (2017).

[203] *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir.) (*citing Khan v. Children's National Health System*, 188 F. Supp. 3d 524, 533 (D. Md. 2016) (holding that "general allegations . . . that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft" was insufficient to establish "substantial risk" of harm); *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig*., 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (finding no "substantial risk" of harm where "[b]y Plaintiff's own calculations, then, injury is likely not impending for over 80% of victims")), *cert denied,* 137 S. Ct. 2307 (2017).

[204] *Beck v. McDonald*, 848 F.3d 262, 275 n.9 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

[205] *See Galaria v. Nationwide Mutual Insurance Co.,* 663 F. App'x 384, 388 (6th Cir. 2016) ("Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year."); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015) ("It is telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all [potentially affected] customers. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.").

breach victims, lest their extension of goodwill render them subject to suit.[206]

The Fourth Circuit panel similarly rejected plaintiffs' allegation that they suffered injury-in-fact because they incurred, or would in the future incur, costs to mitigate the risk of identity theft. The court explained that, as in *Clapper,* the plaintiffs in *Beck* sought " 'to bring this action based on costs they incurred in response to a speculative threat," . . . But this allegation is merely 'a repackaged version of [Plaintiffs'] first failed theory of standing.' . . . Simply put, these self-imposed harms cannot confer standing."[207]

In *In re SuperValu, Inc., Customer Data Security Breach Litigation*,[208] the Eighth Circuit affirmed the dismissal for lack of standing of the claims of 15 of the 16 plaintiffs but held that the one plaintiff who alleged he suffered a fraudulent charge on his credit card had standing to sue for negligence, breach of implied contract, state consumer protection and security breach notification laws and unjust enrichment.[209] In *SuperValu,* the defendants experienced two separate security breaches, which they announced in press

---

[206]*Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir.) (footnote omitted), *cert denied,* 137 S. Ct. 2307 (2017). The court further explained that it

> read *Clapper*'s rejection of the Second Circuit's attempt to import an "objectively reasonable likelihood" standard into Article III standing to express the commonsense notion that a threatened event can be "reasonabl[y] likel[y]" to occur but still be insufficiently "imminent" to constitute an injury-in-fact. *See* 133 S. Ct. at 1147–48. Accordingly, neither the VA's finding that a "reasonable risk exists" for the "potential misuse of sensitive personal information" following the data breaches, nor its decision to pay for credit monitoring to guard against it is enough to show that the Defendants subjected the Plaintiffs to a "substantial risk" of harm.

Beck v. McDonald, 848 F.3d at 276.

[207]*Beck v. McDonald*, 848 F.3d 262, 276-77 (4th Cir.) (*quoting Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409, 416 (2013)), *cert denied,* 137 S. Ct. 2307 (2017); *see also, e.g., Reilly v. Ceridian Corp*., 664 F.3d 38, 46 (3d Cir. 2011) ("[P]rophylactically spen[ding] money to ease fears of [speculative] future third-party criminality . . . is not sufficient to confer standing."), *cert. denied*, 566 U.S. 989 (2012).

[208]*In re SuperValu, Inc., Customer Data Security Breach Litig*., 870 F.3d 763 (8th Cir. 2017).

[209]*In re SuperValu, Inc., Customer Data Security Breach Litig*., 870 F.3d 763, 772-73 (8th Cir. 2017). The court explained that for purposes of merely alleging standing at the pleadings stage, all that was required was a showing of general, not proximate causation. *Id.* at *7 (citing *Lexmark Int'l, Inc. v. Static Control Components, Inc.,*134 S. Ct. 1377, 1391 n.6 (2014) ("Proximate causation is not a requirement of Article III standing.")).

releases may have resulted in the theft of credit card information, including their customers' names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs). Plaintiffs alleged that hackers gained access to defendants' network because defendants failed to take adequate measures to protect customers' credit card information.[210] They also alleged that they had shopped at defendants' stores and their card information had been compromised.

Eighth Circuit Judge Jane Kelly, writing for herself, Chief Judge Lavenski R. "Vence" Smith and Judge Steven Colloton, rejected plaintiffs' argument that the theft of their card information in the data breaches at defendants' stores created a substantial risk that they would suffer identity theft in the future. The court explained that while the Supreme Court has made clear that future injury can be sufficient to establish Article III standing, it is only sufficient where a plaintiff can demonstrate that (a) a threatened injury is "certainly impending" or (b) there is a "substantial risk" that the harm will occur.[211]

The court accepted the proposition that the complaint alleged that the malware that hackers installed on defendants' network plausibly allowed them to "harvest" plaintiffs' card information and that defendants' security practices allowed and made possible the theft. Among other things, the court pointed to defendants' own press release stating that the

---

[210]Plaintiffs alleged that:

> Defendants used default or easily guessed passwords, failed to lock out users after several failed login attempts, and did not segregate access to different parts of the network or use firewalls to protect Card Information. By not implementing these measures, defendants ran afoul of best practices and industry standards for merchants who accept customer payments via credit or debit card. Moreover, defendants were on notice of the risk of consumer data theft because similar security flaws had been exploited in recent data breaches targeting other national retailers.

In re SuperValu, Inc., Customer Data Security Breach Litig., 870 F.3d 763, 766 (8th Cir. 2017).

[211]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 769 & n.3 (8th Cir. 2017) (explaining that "[t]he Supreme Court has at least twice indicated that both the 'certainly impending' and 'substantial risk' standards are applicable in future injury cases, albeit without resolving whether they are distinct, and we are obligated to follow this precedent.") (citing *Susan B. Anthony List v. Driehaus,* 134 S. Ct. 2334, 2341 (2014); *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409, 414 n.5 (2013)).

data breaches "may have" resulted in the theft of card information. But the court held that this was insufficient to establish future harm because plaintiffs had not alleged that their card information had actually been misused. The court rejected allegations made "on information and belief" that their information was being resold online as mere speculation and in any case held that it was insufficient to establish injury because there was no allegation that the information—even if stolen by hackers as a result of defendants' security practices—was being misused.[212]

Judge Kelly rejected plaintiffs' argument that future harm could be inferred from a 2007 U.S. Government Accountability Office (GAO) report. The court noted that the allegedly stolen credit and debit card information "did not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers" and that card information generally cannot be used alone to open unauthorized new accounts.[213] While stolen card data could be used to commit credit or debit card fraud, the GAO report did not "plausibly support the contention that consumers affected by a data breach face a substantial risk of credit or debit card fraud."[214] The GAO report concluded that "based on the 'available data and information . . . most breaches have not resulted in detected incidents of identity theft.' "[215] Accordingly, the court found there was no standing, explaining that "a mere possibility is not enough for standing."[216]

The Eighth Circuit panel also rejected the argument that the costs incurred to mitigate the risk of identity theft,

---

[212]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 770 (8th Cir. 2017) (citing *Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1548 (2016) (holding that injury "must affect the plaintiff in a personal and individual way") (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 n.1 (1992)).

[213]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 770 (8th Cir. 2017).

[214]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 770 (8th Cir. 2017).

[215]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 770 (8th Cir. 2017) (citing the GAO Report).

[216]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 770 (8th Cir. 2017) (citing *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409 (2013) (" '[A]llegations of possible future injury' are not sufficient.") (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990))); *Braitberg v. Charter Communications, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) ("[A] speculative or hypothetical risk is insufficient.").

including the time they spent reviewing information about the breach and monitoring their account information, constituted an injury in fact. The court wrote that, "[b]ecause plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury."[217]

In 2018, the Ninth Circuit, in *In re Zappos.com, Inc.*,[218] reaffirmed its pre-*Clapper* liberal rule of standing from *Krottner v. Starbucks Corp.*,[219] in an opinion focused primarily on *Krottner,* which largely ignored the existing circuit split over the proper standard for establishing standing in a case based on the threat of future harm. In *Zappos,* Circuit Judge Michelle T. Friedland, on behalf of herself, Circuit Judge John B. Owen, and Northern District of Illinois Judge Elaine E. Bucklo, sitting by designation, held that plaintiffs, whose information had been stolen by a hacker but who had not been victims of identity theft or financial fraud, nevertheless had Article III standing to maintain suit in federal court, relying on the fact that other parties had alleged financial harm from the same security breach, which the court found evidenced the risk to these plaintiffs, who did not allege similar harm but alleged the threat of future harm, faced a similar risk. Judge Friedland also cited, in support of standing, the fact that, after the breach, Zappos provided routine post-breach precautionary advice to its customers about changing passwords, which the panel considered to be an acknowledgement by Zappos that the information taken gave the hackers the means to commit financial fraud or identity theft.

Zappos reflects a kind of bootstrapping argument that appears to be inconsistent with *Clapper* and *Spokeo.* The fact that *other people* incurred a financial loss in reality doesn't

---

[217]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763, 771 (8th Cir. 2017) (citing *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 402 (2013) (holding that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending"); *Beck v. McDonald*, 848 F.3d 262, 276-77 (4th Cir.) ("[S]elf-imposed harms cannot confer standing."), *cert denied,* 137 S. Ct. 2307 (2017)).

[218]*In re Zappos.com, Inc.,* 888 F.3d 1020, 1023-30 (9th Cir. 2018).

[219]*Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010) (holding that employees had standing to sue based on their increased risk of future identity theft where a company laptop containing the unencrypted names, addresses, and social security numbers of 97,000 Starbucks employees had been stolen).

make it more likely that the plaintiffs in *Zappos* would as well.

In ruling as it did, the panel distinguished the Fourth Circuit's admonition in *Beck v. McDonald*[220] that the threat of injury from a security breach diminishes with the passage of time, crediting instead plaintiff's mere allegation in its complaint that a person whose PII has been obtained and compromised may not see the full extent of identity theft or identity fraud for years.[221]

The panel noted in a footnote that its interpretation that "*Krottner* is not clearly irreconcilable with *Clapper*" was consistent with the D.C. Circuit's holding in *Attias,* also citing in the same footnote the Seventh Circuit's *Remijas* ruling, while distinguishing the Eighth Circuit's decision in *SuperValu* as one that involved a credit card theft, not the theft of plaintiff's addresses, telephone numbers, or passwords (although, as noted, *Zappos* immediately alerted users to change their passwords so the risk of financial loss or identity theft was likely negligible).[222]

Zappos ultimately reflects the Ninth Circuit's very liberal, pre-*Clapper* standing rule, and is difficult to harmonize with *Clapper*.

While *SuperValu, Beck* and *Whalen* are consistent with Supreme Court precedent (primarily *Clapper*) they are inconsistent with Seventh, Ninth and D.C. Circuit precedents (and an unreported Sixth Circuit opinion following Seventh Circuit law) which applied the circular logic that if information was targeted, the data thieves must have intended to use it, thereby causing a risk of future harm. In fact, many people have their information exposed without becoming victims of identity theft. Similarly, even where attempts are made, they may not be successful because credit card companies often cancel cards quickly and because consumers themselves can put credit freezes on their own accounts substantially reducing the risk of identity theft. Many cyberthefts are opportunistic, with a hacker taking whatever information is available. Even where thieves target specific

---

[220]*Beck v. McDonald,* 848 F.3d 262 (4th Cir.), *cert denied,* 137 S. Ct. 2307 (2017).

[221]*In re Zappos.com, Inc.,* 888 F.3d 1020, 1028-29 & n.13 (9th Cir. 2018).

[222]*In re Zappos.com, Inc.,* 888 F.3d 1020, 1026 n.6 (9th Cir. 2018).

information, simply acquiring it is not the same as being able to use it—especially when the data taken is credit card information that is usually canceled quickly following a breach, or information that is encrypted where the encryption key was not compromised.

The Seventh Circuit's holding (which was also followed by a nonprecedential opinion in the Sixth Circuit) that a company's offer of credit monitoring services to customers evidences that a breach raises more than a de minimis risk of identity theft likewise has been expressly rejected by the Fourth Circuit. More fundamentally, the Second, Fourth and Eighth Circuits expressly hold, consistent with *Clapper,* that mitigation costs and expenses cannot on their own establish standing if they are incurred to prevent a threat that itself is merely hypothetical or speculative. Companies may offer credit monitoring for a host of reasons, including maintaining good customer relations.[223]

While some conflicting court opinions potentially may be harmonized based on whether an attack was intentional or seems likely to lead to identity theft or because of the nature of the information taken (social security numbers vs. credit card numbers, for example), fundamentally the Sixth, Seventh, Ninth, and D.C. Circuits take a more liberal view of when the threat of future identity theft or financial harm justifies standing than the Third, Fourth, and Eighth Circuits (and the Second Circuit in a non-precedential opinion).

In addition to circuit courts, a number of district courts have dismissed security breach cases for lack of standing, on various grounds, since *Spokeo*.[224]

---

[223]Credit monitoring also may be required in the event of a breach pursuant to certain state laws. *See infra* § 27.08.

[224]*See, e.g., Antman v. Uber Technologies, Inc*., Case No. 3:15-cv-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018) (dismissing, with prejudice, plaintiff's claims, arising out of a security breach, for allegedly (1) failing to implement and maintain reasonable security procedures to protect Uber drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract, for lack of Article III standing, where plaintiff could not allege injury sufficient to establish Article III standing); *In re U.S. Office of Personnel Management Data Security Breach Litig.*, 266 F. Supp. 3d 1, 19-26 (D.D.C. 2017) (holding that Federal

Causation and Proof of Harm

Even where standing is established, security breach claims based on potential future harm have proven difficult to maintain, and subject to early motions to dismiss, in the absence of any injury in either state[225] or federal appellate[226]

---

employees did not have standing to sue over a cybersecurity breach by a contractor of the U.S. Office of Personnel Management, which had exposed the names, birthdates, current and former addresses and Social Security numbers of more than twenty-one million people; "While one could make a compelling argument that . . . ["the release or theft of private information—as opposed to any actual or even threatened misuse of that information—is itself the injury in fact for standing purposes"], the Court is not writing a law review article. Therefore, it cannot ignore the fact that neither the Supreme Court nor the D.C. Circuit has embraced this categorical approach to standing . . . ."); *Fero v. Excellus Health Plan, Inc*., 236 F. Supp. 3d 735, 747-56 (W.D.N.Y. 2017) (dismissing without leave to amend but without prejudice in the event they later were subject to identity theft, the claims of the four plaintiffs whose information had been exposed but who had not been subject to identity theft, because allegations of increased risk of identity theft were too speculative to constitute injury-in-fact and alleged mitigation efforts directed at future harm, overpayment for health insurance because of an implied promise to provide data security and diminution of value of their personal information did not constitute injury-in-fact); *Khan v. Children's Nat'l Health System*, 188 F. Supp. 3d 524, 539-34 (D. Md. 2016) (dismissing for lack of standing under *Spokeo* the claims of a patient whose information had been compromised when hackers accessed the email accounts belonging to a number of hospital employees, which gave them access to patients' names, addresses, birthdates, social security numbers, telephone numbers, and private health care information, because the plaintiff did not identify "any potential damages arising from such a loss and thus fails to allege a concrete and particularized injury.").

[225]*See, e.g., Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 708–11 (D.C. 2009) (dismissing claims by participants against a plan administrator for negligence, gross negligence and breach of fiduciary duty because participants did not suffer any actual harm as a result of the theft of a laptop computer, and for invasion of privacy because plaintiff's allegation that defendants failed to implement adequate safeguards did not support a claim for intentional misconduct); *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 455 Mass. 458, 918 N.E.2d 36 (Mass. 2009) (affirming dismissal of contract and negligence claims and summary judgment on the remaining issuing credit unions' claims against a retailer that had improperly stored data from individual credit cards in a manner that allowed thieves to access the data, and against the retailer's acquiring bank that processed the credit card transactions, where the credit unions were not third-party beneficiaries to the agreements between the retailer and acquiring bank, plaintiffs' negligence claims were barred by the economic loss doctrine, the retailer made no fraudulent representations and the credit unions could not have reasonably relied on any

negligent misrepresentations); *Paul v. Providence Health System–Oregon*, 351 Or. 587, 273 P.3d 106, 110–11 (Or. 2012) (affirming dismissal of claims for negligence and a violation of Oregon's Unlawful Trade Practices Act (UTPA) in a putative class action suit arising out of the theft from a health care provider's employee's car of digital records containing patients' personal information where credit monitoring costs, as incurred by patients to protect against the risk of future economic harm in form of identity theft, were not recoverable from the provider as economic damages; patients could not recover damages for negligent infliction of emotional distress based on future risk of identity theft, even if provider owed a duty based on physician-patient relationship to protect patients from such emotional distress; and credit monitoring costs were not a compensable loss under UTPA).

[226]*See, e.g.*, *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012) (affirming dismissal of a brokerage accountholder's putative class action suit alleging that the clearing broker charged fees passed along to accountholders for protecting electronically stored non-public personal information that in fact was vulnerable to unauthorized access, because the accountholder was not a third party beneficiary of the data confidentiality provision of the clearing broker's contract with its customers, the disclosure statement that the broker sent to accountholders did not support a claim for implied contract in the absence of consideration and plaintiff could not state a claim for negligence in the absence of causation and harm, in addition to holding that the plaintiff did not have Article III standing to allege claims for unfair competition and failure to provide notice under Massachusetts law); *In re TJX Cos. Retail Security Breach Litig.*, 564 F.3d 489 (1st Cir. 2009) (affirming, in a security breach case arising out of a hacker attack, dismissal of plaintiffs' (1) negligence claim based on the economic loss doctrine (which holds that purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage) and rejecting the argument that plaintiffs had a property interest in payment card information, which the security breach rendered worthless, because the loss at issue was not the result of physical destruction of property; and (2) breach of contract claim, because plaintiffs were not intended beneficiaries of the contractual security obligations imposed on defendant Fifth Third Bank by VISA and MasterCard; but reversing the lower court's dismissal of plaintiff's unfair competition claim and affirming the lower court's order denying defendant's motion to dismiss plaintiff's negligent misrepresentation claim, albeit with significant skepticism that the claim ultimately would survive); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162 (3d Cir. 2008) (dismissing the issuer bank's negligence claim against a merchant bank for loss resulting from a security breach based on the economic loss doctrine, and the bank's claim for indemnification, in a suit brought to recover the costs incurred to issue new cards and reimburse cardholders for unauthorized charges to their accounts; and reversing summary judgment for the defendant because of a material factual dispute over whether Visa intended to give Sovereign Bank the benefit of Fifth Third Bank's promise to Visa to ensure that merchants, including BJs, complied with provisions of the Visa-Fifth Third Member Agreement prohibiting merchants from

and district[227] courts. While a company may have a contrac-

---

retaining certain credit card information); *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803 (7th Cir. 2018) (affirming dismissal of the banks' putative class action suit against merchants, where the economic loss rule barred plaintiffs' tort claims, the merchants' failure to adopt adequate security measures was not negligence *per se*, merchants were not unjustly enriched, and the banks could not recover under a third party beneficiary theory, among other things); *Stollenwerk v. Tri–West Health Care Alliance*, 254 F. App'x 664, 666–68 (9th Cir. 2007) (affirming summary judgment on claims for damages for credit monitoring services under Arizona law entered against two plaintiffs whose names, addresses and Social Security numbers were stored on defendant's stolen computer servers but who "produced evidence of neither significant exposure of their information nor a significantly increased risk that they will be harmed by its misuse" and reversing summary judgment granted against a third plaintiff who had presented evidence showing a causal relationship between the theft of data and instances of identity theft).

[227]*See, e.g.*, *In re Yahoo! Inc. Customer Data Security Breach Litig.*, 313 F. Supp. 3d 1113, 1143-45 (N.D. Cal. 2018) (dismissing plaintiffs' section 1798.81.5 claim); *Moyer v. Michael's Stores, Inc.*, No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (dismissing claims for breach of implied contract and state consumer fraud statutes based on Michael's alleged failure to secure their credit and debit card information during in-store transactions); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 661–63 (S.D. Ohio 2014) (dismissing plaintiff's invasion of privacy claim under Ohio law in a part of the decision that was not appealed to the Sixth Circuit, which subsequently reversed the district court's holding that the plaintiff lacked standing to assert FCRA, negligence and bailment claims; the district court had found that the plaintiff had standing to sue for invasion of privacy but did not state a claim); *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 963–1014 (S.D. Cal. 2014) (dismissing Fair Credit Reporting Act, negligence (based on a duty to timely disclose the intrusion and duty to provide reasonable security), negligent misrepresentation/omission, breach of implied warranty (as disclaimed by Sony's user agreements), unjust enrichment and claims under the New York Deceptive Practices Act, Ohio and Texas law and for damages (but not injunctive and declaratory relief under) the Michigan Consumer Protection Act); *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 962 (S.D. Cal. 2012) (dismissing plaintiffs' negligence claims under the economic loss rule and as barred by a provision of California's "Shine the Light" law and dismissing plaintiffs' claim for bailment because personal information could not be construed as property that was somehow "delivered" to Sony and expected to be returned, and because the information was stolen as a result of a criminal security breach); *Holmes v. Countrywide Financial Corp.*, No. 5:08-CV-00205-R, 2012 WL 2873892 (W.D. Ky. July 12, 2012) (holding that plaintiffs had standing to maintain suit over the theft of sensitive personal and financial customer data by a Countrywide employee but dismissing claims for lack of injury in a "risk-of-identity-theft" case because "an increased threat of an injury that may never materialize cannot satisfy the injury requirement" under Kentucky

or New Jersey law and credit monitoring services and "the annoyance of unwanted telephone calls" and telephone cancellation fees were not compensable; dismissing claims for unjust enrichment (where no benefit was conferred on Countrywide by the breach), common law fraud (where no damages were incurred in reliance on Countrywide), breach of contract (because of the absence of direct financial harm), alleged security breach notification, consumer fraud and Fair Credit Reporting Act violations and civil conspiracy); *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.,* M.D.L. No. 09-2146, Civil Action No. H-10-171, 2012 WL 896256 (S.D. Tex. Mar. 14, 2012) (dismissing with prejudice plaintiffs' breach of contract claim where the financial institution plaintiffs could not allege that they were intended beneficiaries of Heartland's third party contracts containing confidentiality provisions and dismissing with prejudice plaintiffs' breach of fiduciary duty claim because of the absence any joint venture relationship); *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699 (N.D. Ill. 2012) (dismissing without prejudice claims for common law negligence and negligence *per se* and violations of the Illinois Consumer Fraud Act brought in a putative class action suit against a company that stored personal health information, where plaintiff alleged that the company failed to implement adequate safeguards to protect plaintiff's information and notify him properly when a computer hard drive containing that information was stolen, because the costs associated with the increased risk of identity theft are not legally cognizable under Illinois law); *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566 (S.D. Tex. 2011) (dismissing the financial institution plaintiffs' claims for: (1) breach of contract and breach of implied contract, with leave to amend, but only to the extent plaintiffs could assert in good faith that they were third party beneficiaries of agreements with Heartland and that those agreements did not contain damage limitation provisions that waived claims for indirect, special, exemplary, incidental or consequential damages and limited Heartland's liability to correct any data in which errors had been caused by Heartland; (2) negligence, with prejudice, based on the economic loss doctrine; (3) misrepresentation, with leave to amend to address factually concrete and verifiable statements, rather than mere puffery, made prior to, rather than after the security breach, to the extent relied upon by plaintiffs; (4) implied contract, with prejudice, because "it is unreasonable to rely on a representation when . . . a financial arrangement exists to provide compensation if circumstances later prove the representation false"; (5) misrepresentation based on a theory of nondisclosure, with leave to amend, but only for verifiable factual statements that were actionable misrepresentations, and on which plaintiffs relied; and (6) unfair competition claims asserted under the laws of 23 states, with leave to amend under California, Colorado, Illinois and Texas law (and denying defendant's motion to dismiss plaintiffs' claim under the Florida Deceptive and Unfair Trade Practices Act)), *rev'd in part sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013) (holding that the economic loss doctrine did not bar issuer banks' negligence claims under New Jersey law and does not bar tort recovery in every case where the plaintiff suffers economic harm without any attendant physical harm because (1) the Issuer Banks constituted an "identifi-

able class," Heartland had reason to foresee that the Issuer Banks would be the entities to suffer economic losses were Heartland negligent, and Heartland would not be exposed to "boundless liability," but rather to the reasonable amount of loss from a limited number of entities; and (2) in the absence of a tort remedy, the Issuer Banks would be left with no remedy for Heartland's alleged negligence, defying "notions of fairness, common sense and morality"); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 525–32 (N.D. Ill. 2011) (dismissing plaintiffs' negligence and negligence *per se* claims under the economic loss doctrine which bars tort claims based solely on economic losses; dismissing plaintiffs' Stored Communications Act claim; dismissing plaintiffs' Illinois Consumer Fraud and Deceptive Business Practices Act claim based on deceptive practices because plaintiffs could not identify a specific communication that allegedly failed to disclose that the defendant had allegedly failed to implement adequate security measures, but allowing the claim to the extent based on unfair practices in allegedly failing to comply with Visa's Global Mandate and PCI Security requirements and actual losses in the form of unauthorized bank account withdrawals, not merely an increased risk of future identity theft and costs of credit monitoring services, which do not satisfy the injury requirement; and denying plaintiffs' motion to dismiss claims under the Illinois Personal Information Protection Act (based on the alleged failure to provide timely notice of the security breach) and for breach of implied contract); *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.,* M.D.L. No. 09-2146, Civil Action No. H-10-171, 2011 WL 1232352 (S.D. Tex. Mar. 31, 2011) (dismissing with prejudice financial institution plaintiffs' claims against credit card processor defendants for negligence, based on the economic loss doctrine, and dismissing without prejudice claims for breach of contract (alleging third party beneficiary status), breach of fiduciary duty and vicarious liability); *Hammond v. Bank of N.Y. Mellon Corp.,* No. 08–6060, 2010 WL 2643307, at *4, *7 (S.D.N.Y. June 25, 2010) (finding no standing and, in the alternative, granting summary judgment on plaintiff's claims for negligence, breach of fiduciary duty, implied contract (based on the absence of any direct relationship between the individuals whose data was released and the defendant) and state consumer protection violations based on, among other things, the absence of any injury, in a case where a company owned by the defendant allegedly lost computer backup tapes that contained the payment card data of 12.5 million people); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908 (N.D. Cal. 2009) (holding that a job applicant whose personal information had been stored on a laptop of the defendant's that had been stolen had standing to sue but granting summary judgment for the defendant where the risk of future identity theft did not rise to the level of harm necessary to support plaintiff's negligence claim, which under California law must be appreciable, non-speculative, and present; breach of contract claim, which requires a showing of appreciable and actual harm; unfair competition claim, where an actual loss of money or property must be shown; or claim for invasion of privacy under the California constitution, which may not be premised on the mere risk of an invasion or accidental or negligent conduct by a defendant), *aff'd mem.,* 380 F. App'x 689 (9th Cir. 2010); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605 (S.D.N.Y. 2009) (dismissing plaintiff's negligent misrepresentation

claim under the economic loss doctrine and dismissing claims for violations of N.Y. Gen. Bus. L. § 349, breach of fiduciary duty and breach of contract for the alleged disclosure of plaintiff's email address and the potential dissemination of certain personal information from his bank account with the defendant bank for failure to plead actual injury or damages because "the release of potentially sensitive information alone, without evidence of misuse, is insufficient to cause damage to a plaintiff . . . , the risk of some undefined future harm is too speculative to constitute a compensable injury" and the receipt of spam by itself does not constitute a sufficient injury); *Pinero v. Jackson Hewitt Tax Service Inc.*, 594 F. Supp. 2d 710 (E.D. La. 2009) (holding that the mere possibility that personal information was at increased risk did not constitute an actual injury sufficient to state claims for fraud, breach of contract (based on emotional harm), negligence, or a violation of the Louisiana Database Security Breach Notification Law (because disposal of tax records in paper form in a public dumpster, which were not burned, shredded or pulverized, did not involve computerized data) but holding that the plaintiff had stated a claim for invasion of privacy and had alleged sufficient harm to state a claim under the Louisiana Unfair Trade Practices Act (but had not alleged sufficient particularity to state a claim under that statute)); *McLoughlin v. People's United Bank, Inc.,* No. Civ A 308CV-00944 VLB, 2009 WL 2843269 (D. Conn. Aug 31, 2009) (dismissing plaintiff's claims for negligence and breach of fiduciary duty); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273 (S.D.N.Y. 2008) (holding that plaintiff had standing to sue his employer's pension consultant, seeking to recover the costs of multi-year credit monitoring and identity theft insurance, following the theft of a laptop containing his personal information from the consultant's office, and denying defendant's motion to dismiss his breach of contract claim premised on being a third party beneficiary of a contract between his employer and the consultant, but dismissing claims for negligence and breach of fiduciary duty under New York law because the plaintiff lacked a basis for a serious concern over the misuse of his personal information and New York would not likely recognize mitigation costs as damages without a rational basis for plaintiffs' fear of misuse of personal information); *Melancon v. Louisiana Office of Student Fin. Assistance*, 567 F. Supp. 2d 873 (E.D. La. 2008) (granting summary judgment for Iron Mountain in a security breach putative class action suit arising out of the loss of backup data from an Iron Mountain truck because the mere possibility that personal student financial aid information may have been at increased risk did not constitute an actual injury sufficient to maintain a claim for negligence); *Shafran v. Harley–Davidson, Inc.*, No. 07 C 1365, 2008 WL 763177 (S.D.N.Y. Mar. 24, 2008) (dismissing claims for negligence, breach of warranty, unjust enrichment, breach of fiduciary duty, violation of N.Y. Gen. Bus. Law § 349, violation of N.Y. Gen. Bus. Laws §§ 350, 350-a and 350e, fraudulent misrepresentation, negligent misrepresentation, *prima facie* tort, and breach of contract, in a putative class action suit based on the loss of personal information of 60,000 Harley Davidson owners whose information had been stored on a lost laptop, because under New York law, the time and money that could be spent to guard against identity theft does not constitute an existing compensable injury; noting that "[c]ourts have uniformly ruled that the time and

tual claim against a third party vendor responsible for a security breach, consumer contracts rarely provide such assurances and individuals usually are not intended beneficiaries of corporate security contracts with outside vendors.[228] Some representations to consumers about a company's security practices also may be viewed as merely puffery.[229]

---

expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy."); *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 797–98 (M.D. La. 2007) (dismissing a putative class action suit alleging that a nine week delay in providing notice that personal information on 17,000 current and former employees had been compromised when an employee installed file sharing software on his company-issued laptop violated Louisiana's Database Security Breach Notification Law because the plaintiff could only allege emotional harm in the form of fear and apprehension of fraud, loss of money and identity theft, but no "actual damage" within the meaning of Louisiana law); *Hendricks v. DSW Shoe Warehouse Inc.*, 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) (dismissing claims under the Michigan Consumer Protection Act and for breach of contract arising out of a security breach because "[t]here is no existing Michigan statutory or case law authority to support plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss."); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1020–21 (D. Minn. 2006) (granting summary judgment for the defendant on plaintiffs' claims for negligence and breach of contract in a security breach case arising out of the theft of a Wells Fargo computer on which their personal information had been stored, where the plaintiffs could not show any present injury or reasonably certain future injury and the court rejected plaintiffs' contention that they had suffered damage as a result of the time and money they had spent to monitor their credit).

[228]*See, e.g.*, *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012) (holding that an account holder was not a third party beneficiary of a data confidentiality provision of the clearing broker's contract with its customers); *Sackin v. Transperfect Globalm Inc.*, 278 F. Supp. 3d 739 (S.D.N.Y. 2017) (dismissing employees' claim for breach of express contract but allowing claims for negligence under New York law and breach of implied contract to proceed, in a suit arising out of a security breach of the employer's computer system that caused the disclosure of sensitive personally identifiable information).

[229]*See Cheatham v. ADT Corp.*, 161 F. Supp. 3d 815, 828 (D. Ariz. 2016) (holding that representations that ADT's security system "protects against unwanted entry and property loss" and provides "reliable security protection" were factual assertions but certain claims made by ADT about the efficacy of its wireless security system were puffery; "For example, the company's claim that its system provides 'worry-free' living . . . is a statement of opinion, not fact. This claim is not amenable to general verification or falsification because its truth or falsity for a particular consumer depends as much on the characteristics of that consumer as the efficacy of the product.").

Negligence claims likewise typically fail based on the economic loss doctrine, which holds that purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage. Breach of fiduciary duty claims also often fail in the absence of a fiduciary obligation. Breach of contract, breach of implied contract and unfair competition claims likewise may fail where there has been no economic loss. Claims based on delay in providing notification also may fail in the absence of any actual injury proximately caused by the alleged delay.[230]

Claims based on negligence or a failure to warn consumers also potentially may be preempted by the Cybersecurity Information Sharing Act (CISA),[231] where companies learned of a threat as a result of voluntarily sharing information with other companies or the government or by monitoring their own systems. Among other things, CISA provides that "[n]o cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information" pursuant to the statute.[232] The CISA also creates an exemption from liability for sharing or receiving cyber threat indicators after December 18, 2015, pursuant to the terms of the Act.[233] If applicable, CISA "supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this subchapter."[234]

State law may provide a defense for businesses with written information security programs. For example, Ohio's cybersecurity law provides a defense to certain tort actions brought in Ohio state courts or under Ohio law that allege that the failure to implement reasonable information secu-

---

[230]*See, e.g., In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (dismissing plaintiffs' claim for alleged delay in providing consumer notice where there was no traceable harm); *In re Barnes & Noble Pin Pad Litig.,* 12-CV-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (rejecting the argument that the delay or inadequacy of breach notification increased plaintiffs' risk of injury).

[231]6 U.S.C.A. §§ 1501 to 1510; *see generally supra* § 27.04[1.5] (analyzing the statute).

[232]6 U.S.C.A. § 1505(a); *supra* § 27.04[1.5].

[233]*See* 6 U.S.C.A. § 1505(b); *supra* § 27.04[1.5].

[234]*See* 6 U.S.C.A. § 1507(k)(1); *supra* § 27.04[1.5].

rity controls resulted in a data breach.[235] The law creates an affirmative defense "to any cause of action sounding in tort" brought under Ohio law or in Ohio courts "that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information[,]" where a *covered entity*[236] has created, maintains, and complies with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information[237] (or the protec-

---

[235]*See* Ohio Rev. Code Ann. §§ 1354.01 to 1354.05; *see generally supra* § 27.04[6][H]. A *data breach* means

> unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to person or property. "Data breach" does not include either of the following:
>
> (1) Good faith acquisition of personal information or restricted information by the covered entity's employee or agent for the purposes of the covered entity's, provided that the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure;
>
> (2) Acquisition of personal information or restricted information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency.

Ohio Rev. Code Ann. § 1354.01(C).

[236]A *covered entity* means "a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state." Ohio Rev. Code Ann. § 1354.01(B). A *business* is defined as "any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing." *Id.* § 1354.01(A).

[237]*Personal information* has the same meaning as in section 1349.19 of the Revised Code. Ohio Rev. Code Ann. § 1354.01(D). Section 1349 defined *personal information* to mean

> (a) . . . an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:
>
> (i) Social security number;
>
> (ii) Driver's license number or state identification card number;

tion of both personal information and restricted information[238]) and that reasonably conforms to an "industry

(iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

(b) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:

(i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;

(ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section;

(iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;

(iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section.

Ohio Rev. Code Ann. § 1349.19(A)(7). *Encrypted*, *individual*, and *redacted* have the same meanings as in section 1349.19 of the Revised Code. *Id.* § 1354.01(E). *Encryption* "means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." Ohio Rev. Code Ann. § 1349.19(A)(4). An *individual* means a natural person. *Id.* § 1349.19(A)(5). *Redacted* means "altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data." *Id.* § 1349.19(A)(9).

[238]*Restricted information* means "any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property." Ohio Rev. Code Ann. § 1354.01(E).

Encrypted, *individual*, and *redacted* have the same meanings as in section 1349.19 of the Revised Code. *Id. Encryption* "means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." Ohio Rev. Code Ann. § 1349.19(A)(4). An *individual* means a natural person. *Id.* § 1349.19(A)(5). *Redacted* means "altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data." *Id.* § 1349.19(A)(9).

recognized cybersecurity framework."[239] It further provides that a covered entity's failure or decision not to comply may not support a private cause of action.[240] The technical requirements for meeting the safe harbor are set forth in greater detail in section 27.04[6][H].[241]

State security breach notification statutes also may provide both potential claims and defenses, as analyzed more extensively in section 27.08[10]. For example, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[242] the court dismissed negligence claims brought by California residents against a company that experienced a security breach because California's security breach notification law, Cal. Civil Code § 1798.84(d), provides that "[u]nless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively."[243] The court reasoned that claims by California residents were barred because plaintiff's Complaint only alleged "that Sony either knew or should have known that its security measures were inadequate, and failed to inform Plaintiffs of the breach in a timely fashion, [and] none of Plaintiffs current allegations assert[ed] willful, intentional,

---

[239]Ohio Rev. Code Ann. § 1354.02(D).

[240]*See* Ohio Rev. Code Ann. § 1354.04.

[241]The statutory provisions creating the Ohio safe harbor are reprinted in section 27.09[38]. Guidelines for drafting a written information security program are set forth in section 27.13.

[242]*In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 973 (S.D. Cal. 2012).

[243]*In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 973 (S.D. Cal. 2012) (quoting the statute); *see generally supra* § 26.13[6][D] (analyzing the statute).

or reckless conduct on behalf of Sony."[244]

In *Sony,* among other rulings, the court also dismissed plaintiffs' claim for bailment, holding that personal information could not be construed as property that was somehow "delivered" to Sony and expected to be returned, and because the information was stolen as a result of a criminal intrusion of Sony's Network.[245]

On the other hand, plaintiffs have had some success getting past motions to dismiss on some state law claims, including state statutory claims, as underscored by the *Sony* case itself. In a later opinion in *Sony*, the court allowed California Consumer Legal Remedies Act and California statutory unfair competition and false advertising law claims to go forward based on the allegations that Sony misrepresented that it would take "reasonable steps" to secure plaintiff's information and that Sony Online Services used "industry-standard encryption to prevent unauthorized access to sensitive financial information" and allegedly omitted to disclose that it did not have reasonable and adequate safeguards in place to protect consumers' confidential information, allegedly failed to immediately notify California residents that the intrusion had occurred and allegedly omitted material facts regarding the security of its network, including the fact that Sony allegedly failed to install and maintain firewalls and use industry-standard encryption. The court also allowed plaintiff to proceed with claims for declaratory and injunctive relief under the Florida Deceptive and Unfair Trade Practices Act, injunctive and declaratory relief under Michigan law and claims under Missouri and New Hamp-

---

[244]*In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 973 (S.D. Cal. 2012); *see also In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *33-40 (N.D. Cal. Aug. 30, 2017) (dismissing California security breach notification claims under the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.* for violations of section 1798.82 brought on behalf of plaintiffs who were not California residents, for lack of standing, and for a failure to provide notice about an older 2013 breach, but denying the motion with respect to claims of California plaintiffs alleging unreasonable delay); *Corona v. Sony Pictures Entertainment*, No. 14–CV–09600 RGK (Ex), 2015 WL 3916744, at *6 (C.D. Cal. June 15, 2015) (dismissing without leave to amend plaintiffs' 1798.84 claim in a suit arising out of the Sony Pictures security breach because plaintiffs did not qualify as "customers" under the California Records Act).

[245]*In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 974–75 (S.D. Cal. 2012).

shire law and allowed claims for injunctive relief under California's security breach notification law, Cal. Civil Code § 1789.84(e) (but not damages under section 1789.84(b)) and partial performance and breach of the implied duty of good faith and fair dealing,[246] even as the court dismissed multiple other claims for negligence, negligent misrepresentation/omission, unjust enrichment and state consumer protection laws.

Effective January 1, 2020, the California Consumer Privacy Act (CCPA)[247] will authorize statutory damages of between $100 and $750 "per consumer per incident or actual damages, whichever is greater," injunctive or declaratory relief, and any other relief that a court deems proper[248] for consumers "whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices . . . ."[249] The ability for plaintiffs to recover statutory damages is likely to increase

---

[246]*In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 985–92 (S.D. Cal. 2014)

[247]Cal. Civ. Code §§ 1798.100 to 1798.199.

[248]Cal. Civ. Code § 1798.150(a)(1).

[249]Cal. Civ. Code § 1798.150(a)(1). *Personal information* in this section is defined by reference section 1798.81.5, which is narrower in scope than the CCPA's definition in section 1798.140(o). *Personal information* under section 1798.81.5 means either of the following:

(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  (i) Social security number.
  (ii) Driver's license number or California identification card number.
  (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
  (iv) Medical information.
  (v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

Cal. Bus. & Prof. Code § 1798.81.5(d)(1). *Personal information* does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records." *Id.* § 1798.81.5(d)(4).

the volume of litigation arising out of security breaches, or perceived security breaches, assuming that the law takes effect in this form as planned. This statutory provision, and the CCPA in general, are analyzed in section 26.13A, which addresses the consequences of the CCPA in litigation.

Where a security breach has led to identity theft, unauthorized charges or other injury, a plaintiff will be more likely to be able to state a claim.[250] For example, in *Anderson v.*

Medical information means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional. *Id.* § 1798.81.5(d)(2).

Health insurance information means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. *Id.* § 1798.81.5(d)(3).

[250]*See, e.g.*, *Anderson v. Hannaford Brothers Co.*, 659 F.3d 151 (1st Cir. 2011) (reversing dismissal of negligence and implied contract claims in a case where the plaintiffs alleged actual misuse of credit card data from others subject to the breach such that they faced a real risk of identity theft, not merely one that was hypothetical); *In re TJX Cos. Retail Security Breach Litig.*, 564 F.3d 489 (1st Cir. 2009) (reversing the lower court's dismissal of plaintiffs' unfair trade practices claim under Massachusetts law based on a company's lack of security measures and FTC unfairness criteria (*supra* § 27.06), where the company's conduct allegedly was systematically reckless and aggravated by a failure to give prompt notice when lapses were discovered internally, which allegedly caused widespread and serious harm to other companies and consumers; and affirming the denial of defendant's motion to dismiss plaintiffs' negligent misrepresentation claim arising from the implied representation that the defendant would comply with MasterCard and VISA's security regulations, albeit with significant skepticism about the ultimate merits of that claim, in an opinion that also affirmed the lower court's dismissal of plaintiffs' claims for negligence and breach of contract); *Stollenwerk v. Tri–West Health Care Alliance*, 254 F. App'x 664, 666–68 (9th Cir. 2007) (reversing summary judgment on claims for damages for credit monitoring services under Arizona law against a plaintiff who had presented evidence showing a causal relationship between the theft of data and instances of identity theft, while affirming summary judgment against two other plaintiffs, all of whose names, addresses and Social Security numbers had been stored on defendant's stolen computer servers); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (holding that victims of identity theft had stated claims for negligence, breach of fiduciary duty, breach of contract, breach of implied contract, and unjust enrichment/restitution, in a suit arising out of the disclosure of sensitive information of 1.2 million current and former AvMed members (including protected health information, Social Security numbers, names, addresses and phone numbers) when two laptops containing unencrypted data were stolen from the

Hannaford Brothers Co.,[251] the First Circuit affirmed dismissal of claims for breach of fiduciary duty, breach of implied warranty, strict liability, failure to notify customers of a data breach and unfair competition, but reversed dismissal of negligence and implied contract claims brought by customers of a national grocery chain whose credit card information was taken, and in some cases used for unauthorized charges, when hackers gained access to up to 4.2 million credit and debit card numbers, expiration dates and security codes (but not customer names) between December 7, 2007 and March 10, 2008. The court held that a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would not use credit card data "for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information."[252] The court explained that:

When a customer uses a credit card in a commercial transac-

---

company's Gainesville, Florida office); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 525–35 (N.D. Ill. 2011) (following *Hannaford* in denying defendant's motion to dismiss plaintiffs' claim for breach of an implied contract which obligated the defendant to take reasonable measures to protect plaintiffs' financial information and notify plaintiffs of a security breach within a reasonable amount of time, in a putative class action suit arising out of a security breach based on skimming credit card information and PIN numbers from PIN pads in defendant's stores; denying defendant's motion to dismiss plaintiffs' claim under the Illinois Personal Information Protection Act for allegedly failing to timely notify affected consumers; denying defendant's motion to dismiss plaintiffs' Illinois Consumer Fraud and Deceptive Business Practices Act claim to the extent based on unfairness in allegedly failing to comply with Visa's Global Mandate and PCI Security requirements and premised on actual losses in the form of unreimbursed bank account withdrawals and fees, but dismissing the claim to the extent based on deceptiveness or merely the increased risk of future identity theft and costs of credit monitoring services or reimbursed withdrawals or fees, which would not satisfy the statute's injury requirement; and dismissing Stored Communications Act, negligence and negligence *per se* claims); *Pinero v. Jackson Hewitt Tax Service Inc.*, 594 F. Supp. 2d 710 (E.D. La. 2009) (holding that the plaintiff had stated a claim for invasion of privacy but dismissing other claims because the mere possibility that personal information was at increased risk did not constitute an actual injury to support plaintiff's other claims); *Dittman v. UPMC*, ___ A.3d ___, 2018 WL 6072199 (Pa. 2018) (reversing dismissal and remanding claims arising out of a security breach where plaintiffs alleged that the release of their information allowed third parties to file fraudulent tax returns in their names, causing them economic loss).

[251]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151 (1st Cir. 2011).

[252]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 159 (1st Cir.

> tion, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.[253]

With respect to plaintiffs' negligence and implied contract claims, the First Circuit distinguished between those claims that sought to recover mitigation costs and those that did not. Holding that Maine law allowed recovery of reasonably foreseeable damages, including the costs and harms incurred during a reasonable effort to mitigate (as judged at the time the decision to mitigate was made), the court held that a jury could find that the purchase of identity theft insurance and the cost for replacement credit cards was reasonable.[254] The appellate panel emphasized that this case involved "a large-scale criminal operation conducted over three months and the deliberate taking of credit and debit card information by sophisticated thieves intending to use the information to their financial advantage."[255] Unlike cases based on inadvertently misplaced or lost data, *Anderson v. Hannaford Brothers Co.* involved actual misuse by thieves with apparent expertise who used the data they stole to run up thousands of improper charges across the globe such that "card owners were not merely exposed to a hypothetical risk, but to a real risk of misuse."[256] The court noted that the fact that many banks and credit card issuers immediately

---

2011).

[253]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 159 (1st Cir. 2011); *see also In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531–32 (N.D. Ill. 2011) (following *Hannaford* in denying defendant's motion to dismiss plaintiffs' claim for breach of an implied contract obligating the defendant to take reasonable measures to protect plaintiffs' financial information and notify plaintiffs of a security breach within a reasonable amount of time, in a putative class action suit arising out of a security breach based on skimming credit card information and PIN numbers from PIN pads in defendant's stores).

[254]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 162–65 (1st Cir. 2011).

[255]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 164 (1st Cir. 2011).

[256]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 164 (1st Cir. 2011). The court noted that most data breach cases involve data that was simply lost or misplaced, rather than stolen, where no known misuse had occurred, and where courts therefore had not allowed recovery of damages, including credit monitoring costs. *See id.* at 166 n.11. The panel also

replaced compromised cards with new ones evidenced the reasonableness of replacing cards to mitigate damage, while the fact that other financial institutions did not issue replacement cards did not make it unreasonable for cardholders to take steps on their own to protect themselves.[257]

On the other hand, the appellate panel agreed with the district court that non-mitigation costs—such as fees for preauthorization changes, the loss of reward points and the loss of reward point earning opportunities—were not recoverable because their connection to the harm alleged was too attenuated and the charges were incurred as a result of third parties' unpredictable responses to the cancellation of plaintiffs' credit or debit cards.[258]

In contrast to plaintiffs' negligence and implied contract claims, the First Circuit affirmed dismissal of plaintiffs' unfair competition claim premised on Hannaford's failure to disclose the data theft promptly and possibly a failure to maintain reasonable security.[259] The court's holding, however, turned on the narrow nature of Maine's unfair competition

---

emphasized that, unlike in *Hannaford,* even prior cases where thieves actually accessed plaintiffs' data held by defendants—*Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007) (where hackers breached a bank website and stole the personal and financial data of tens of thousands of the bank's customers) and *Hendricks v. DSW Shoe Warehouse Inc.*, 444 F. Supp. 2d 775, 777 (W.D. Mich. 2006) (where hackers accessed "the numbers and names associated with approximately 1,438,281 credit and debit cards and 96,385 checking account numbers and drivers' license numbers" that were on file with a national shoe retailer)—had not involved allegations that any member of the putative class *already* had been a victim of identity theft as a result of the breach. *See Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 166 (1st Cir. 2011).

[257]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 164 (1st Cir. 2011). The panel explained:

> It was foreseeable, on these facts, that a customer, knowing that her credit or debit card data had been compromised and that thousands of fraudulent charges had resulted from the same security breach, would replace the card to mitigate against misuse of the card data. It is true that the only plaintiffs to allege having to pay a replacement card fee, Cyndi Fear and Thomas Fear, do not allege that they experienced any unauthorized charges to their account, but the test for mitigation is not hindsight. Similarly, it was foreseeable that a customer who had experienced unauthorized charges to her account, such as plaintiff Lori Valburn, would reasonably purchase insurance to protect against the consequences of data misuse.

Id. at 164–65.

[258]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 167 (1st Cir. 2011).

[259]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 159 (1st Cir.

law, which has been construed to require a showing that a plaintiff suffered a substantial loss of money or property as a result of an allegedly unlawful act.[260]

On remand, the lower court denied plaintiffs' motion for class certification, finding that common questions of law and fact did not predominate.[261]

In *Dittman v. UPMC*,[262] the Pennsylvania Supreme Court held that employers owe employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm in collecting and storing employees' data on computer systems, in a suit arising out of the theft of employee data (including names, birth dates, social security numbers, tax information, addresses, salaries, and bank information) from the University of Pittsburgh Medical Center's computer system, which resulted in third parties filing fraudulent tax returns in plaintiffs' names, causing them actual damage. The court also held that the economic loss doctrine did not bar plaintiffs' negligence claim because purely pecuniary damages are recoverable for negligence under Pennsylvania law where a plaintiff can establish breach of a common law duty, independent of any duty assumed by contract. In holding that plaintiffs stated a claim and finding a legal duty in *Dittman*, the Pennsylvania Supreme Court emphasized that UPMC required its employees to provide sensitive personal information as a condition of employment but then failed to employ adequate safety measures, such as "proper encryption, adequate firewalls, and an adequate authentication protocol" in making this data available on a computer accessible over the Internet.

In contrast to *Hanaford Brothers* and *Dittman*, in *Irwin v. Jimmy John's Franchise LLC*,[263] a district court in Arizona held that a restaurant operator did not have a duty to safeguard customer's personal information under either Illinois or Arizona law. Likewise, in *McConnell v. Georgia*

2011).

[260]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 160 (1st Cir. 2011), *citing McKinnon v. Honeywell Int'l, Inc.*, 977 A.2d 420, 427 (Me. 2009).

[261]*See In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 293 F.R.D. 21 (D. Me. 2013).

[262]*Dittman v. UPMC*, __ A.3d __, 2018 WL 6072199 (Pa. 2018).

[263]*Irwin v. Jimmy John's Franchise LLC*, 175 F. Supp. 3d 1064, 1071 (C.D. Ill. 2016).

Department of Labor,[264] an appellate court in Georgia held that there was no general duty of care to safeguard personal information under Georgia law and none could be inferred from the enactment of Georgia's security breach notification statute or a statute prohibiting use and display of social security numbers. The court also held that plaintiff's breach of fiduciary duty and invasion of privacy tort claims were properly dismissed, where the Department of Labor had sent an email to approximately 1,000 Georgians who had applied for unemployment benefits, which included a spreadsheet that listed the name, social security number, home phone number, email address, and age of over 4,000 state residents, because there was no confidential relationship to support a breach of fiduciary duty claim, and no intrusion on plaintiff's seclusion, to support a common law claim for invasion of privacy.[265]

In *Resnick v. AvMed, Inc.,*[266] the Eleventh Circuit held that victims of identity theft had stated claims for negligence, breach of fiduciary duty, breach of contract, breach of implied contract and unjust enrichment/restitution, in a suit arising out of the disclosure of sensitive information of 1.2 million current and former AvMed members (including protected health information, Social Security numbers, names, addresses and phone numbers) when two laptops containing unencrypted data were stolen from the company's Gainesville, Florida office. The court held, however, that plaintiffs had not stated claims for negligence *per se,* because AvMed was not subject to the statute that plaintiffs' claim was premised upon, or breach of the covenant of good faith and fair dealing, which failed to allege a conscious and deliberate act which unfairly frustrates the agreed common purposes, as required by Florida law.

In *Resnick*, ten months after the laptop theft, identity thieves opened Bank of America accounts in the name of one of the plaintiffs, activated and used credit cards for unauthorized purchases and sent a change of address notice to the U.S. postal service to delay plaintiff learning of the unauthorized accounts and charges. Fourteen months after the theft

---

[264]*McConnell v. Georgia Department of Labor*, 345 Ga. App. 669, 678, 814 S.E.2d 790, 798 (2018).

[265]*McConnell v. Georgia Department of Labor*, 345 Ga. App. 669, 680-82, 814 S.E.2d 790, 800-01 (2018).

[266]*Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012).

a third party opened and then overdrew an account with E*TRADE Financial in the name of another plaintiff.

In ruling that plaintiffs stated claims for relief resulting from identity theft, the court held that plaintiffs adequately pled causation where plaintiffs alleged that they had taken substantial precautions to protect themselves from identity theft (including not transmitting unencrypted sensitive information over the Internet, storing documents containing sensitive information in a safe and secure location and destroying documents received by mail that included sensitive information) and that the information used to open unauthorized accounts was the same information stolen from AvMed. The court emphasized that for purposes of stating a claim, "a mere temporal connection is not sufficient; Plaintiffs' pleadings must indicate a logical connection between the two incidents."[267]

The court also ruled that plaintiffs stated a claim for unjust enrichment, which under Florida law required a showing that (1) the plaintiff conferred a benefit on the defendant, (2) the defendant had knowledge of the benefit, (3) the defendant accepted or retained the benefit conferred, and (4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying for it.[268] Plaintiffs alleged that they conferred a benefit on AvMed in the form of monthly premiums that AvMed should not be permitted to retain because it allegedly failed to implement data management and security measures mandated by industry standards.[269]

Where claims proceed past a motion to dismiss, a central issue in a security breach case may be the reasonableness of a company's practices and procedures. In *Patco Construction Co. v. People's United Bank*,[270] the First Circuit held that the defendant bank's security procedures were not commercially reasonable within the meaning of Maine's implementation of U.C.C. Article 4A, which governs wholesale wire transfers and commercial ACH transfers, generally between busi-

---

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

[268] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012).

[269] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012).

[270] *Patco Construction Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012).

nesses and their financial institutions.[271] *Patco* was a suit brought over six fraudulent withdrawals, totaling $588,851.26, from Patco Construction Co.'s commercial bank account with the defendant. Under Article 4A, a bank receiving a payment ordinarily bears the risk of loss for any unauthorized funds transfer unless a bank can show that the payment order received is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency[272] (which typically cannot be shown when a payment order is transferred electronically) or pursuant to section 4-1202(2), if a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, and, among other things, "[t]he security procedure is a commercially reasonable method of providing security against unauthorized payment orders . . . ."[273]

The First Circuit held that the defendant had failed to employ commercially reasonable security when it lowered the dollar amount used to trigger secondary authentication measures to $1 without implementing additional security precautions. By doing so, the bank required users to answer

---

[271]Consumer electronic payments, such as those made through direct wiring or use of a debit card, are governed by the Electronic Fund Transfer Act, 15 U.S.C.A. §§ 1693 *et seq*. "Article 4A does not apply to any funds transfer that is covered by the EFTA; the two are mutually exclusive." *Patco Construction Co. v. People's United Bank*, 684 F.3d 197, 207 n.7 (1st Cir. 2012).

[272]Me. Rev. Stat. Ann. tit. 11, § 4-1202(1).

[273]Me. Rev. Stat. Ann. tit. 11, § 4-1202(2). Section 4-1202(2) allows a bank to shift the risk of loss to a commercial customer, whether or not a payment is authorized. That section provides:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if:
>
> (a) The security procedure is a commercially reasonable method of providing security against unauthorized payment orders; and
>
> (b) The bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.

Id. § 4–1202(2).

challenge questions for essentially all electronic transactions, increasing the risk that these answers would be compromised by keyloggers or other malware. By increasing the risk of fraud through unauthorized use of compromised security answers, the court held that the defendant bank's security system failed to be commercially reasonable because it did not incorporate additional security measures, such as requiring tokens or other means of generating "one-time" passwords or monitoring high risk score transactions, using email alerts and inquiries or otherwise providing immediate notice to customers of high risk transactions. As the court explained, the bank

> substantially increase[d] the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and high dollar transfers. Then, when it had warning that such fraud was likely occurring in a given transaction, Ocean Bank neither monitored that transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable. We emphasize that it was these collective failures taken as a whole, rather than any single failure, which rendered Ocean Bank's security system commercially unreasonable.[274]

By contrast, in *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*,[275] the Eighth Circuit found a bank's security precautions to be reasonable where the bank (1) required customers, in order to be able to send wire transfers, to register a user id and password, (2) installed device authentication software called PassMark, which recorded the IP address and information about the computer used to first access the system, and thereafter required users to verify their identity by answering "challenge questions" if they accessed the bank from an unrecognized computer, (3) allowed its customers to place dollar limits on the daily volume of wire transfer activity from their accounts, and (4) offered its customers a security measure called "dual control" which created a pending payment order, when a wire transfer order was received, that required a second authorized user to approve, before the order would be processed.

---

[274] *Patco Construction Co. v. People's United Bank*, 684 F.3d 197, 210–11 (1st Cir. 2012).

[275] *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611 (8th Cir. 2014).

Choice had declined to place dollar limits on daily transactions or use dual control. In that case, Choice, in November 2009, received an email from one of its underwriters, describing a phishing scam, which it forwarded to BancorpSouth with a request that wires to foreign banks be limited. BancorpSouth responded two days later advising that it could not restrict foreign transfers but encouraging Choice to implement dual control on wires as the best way to deter fraud. Choice again declined to do so. Thereafter, a Choice employee was the victim of a phishing scam and contracted a virus that gave an unknown third party access to the employee's username and password and allowed the third party to mimic the computer's IP address and other characteristics, leading to an unauthorized transfer of $440,000 from Choice's account to a bank in Cypress. On appeal, the Eighth Circuit affirmed the lower court's entry of judgment for BancorpSouth, finding its security measures to be commercially reasonable within the meaning of Article 4A, as adopted in Mississippi.

Where claims are based on misrepresentations allegedly made about a company's security practices, a court will distinguish actionable statements of fact from mere puffery. Puffery has been described as "vague, highly subjective claims as opposed to specific, detailed factual assertions."[276] For example, in *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*,[277] the court dismissed the financial institution plaintiffs' claims for fraud and misrepresentation against a credit and debit card processor whose computer systems had been compromised by hackers, with leave to amend to allege factually concrete and verifiable statements, rather than mere puffery, made prior to, rather than after the security breach, to the extent relied

---

[276]*In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566, 591 (S.D. Tex. 2011) (quoting an earlier case), *rev'd in part on other grounds sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013) (reversing the lower court's order dismissing plaintiffs' negligence claim); *Haskell v. Time, Inc.*, 857 F. Supp. 1392, 1399 (E.D. Cal. 1994); *see generally supra* § 6.12[5][B] (analyzing puffing in the context of Lanham Act false advertising claims).

[277]*In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566 (S.D. Tex. 2011), *rev'd in part on other grounds sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013) (reversing the lower court's order dismissing plaintiffs' negligence claim).

upon by plaintiffs. In so holding, the court explained the difference between those statements contained in S.E.C. filings, made in analyst calls or posted on Heartland's website which were actionable and those which amounted to mere puffery. The court held that Heartland's slogans—*The Highest Standards* and *The Most Trusted Transactions*—were puffery on which the financial institution plaintiffs could not reasonably rely.[278] The court similarly held that the following statements were not actionable representations:

- that Heartland used "layers of state-of-the-art security, technology and techniques to safeguard sensitive credit and debit card account information";
- that it used the "state-of-the-art [Heartland] Exchange"; and
- that its "success is the result of the combination of a superior long-term customer relationship sales model and the premier technology processing platform in the industry today."[279]

The court clarified that to the extent that Heartland's statements and conduct amounted to a guarantee of absolute data security, reliance would be unreasonable as a matter of law, given widespread knowledge of sophisticated hackers, data theft, software glitches and computer viruses.[280]

On the other hand, it found the following statements to be factual representations that were sufficiently definite, factually concrete and verifiable to support a claim for negligent misrepresentation:

- "We maintain current updates of network and operating system security releases and virus definitions, and

---

[278]*In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566, 592 (S.D. Tex. 2011), *rev'd in part on other grounds sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013) (reversing the lower court's order dismissing plaintiffs' negligence claim).

[279]*In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566, 592 (S.D. Tex. 2011), *rev'd in part on other grounds sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013) (reversing the lower court's order dismissing plaintiffs' negligence claim).

[280]*In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566, 592 (S.D. Tex. 2011), *rev'd in part on other grounds sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013) (reversing the lower court's order dismissing plaintiffs' negligence claim).

have engaged a third party to regularly test our systems for vulnerability to unauthorized access."

- "We encrypt the cardholder numbers that are stored in our databases using triple-DES protocols, which represent the highest commercially available standard for encryption."
- Heartland's "Exchange has passed an independent verification process validating compliance with VISA requirements for data security."[281]

Security breaches also may raise breach of contract questions where one party fails to perform or pays the wrong entity as a result of a security breach or phishing scam.[282]

Despite the prevalence of security breaches, the volume of security breach class action litigation has not been as large as one might expect. Indeed, despite the potential for more substantial economic harm when a security breach occurs, there has not been an explosion of security breach class action suits to rival the large number of data privacy suits

---

[281] *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566, 593–94 (S.D. Tex. 2011), *rev'd in part on other grounds sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013) (reversing the lower court's order dismissing plaintiffs' negligence claim). The court also found the following statements to constitute representations about Heartland's privacy practices that, while not puffery, were not relevant to the data breach at issue in the case:

- "we have limited our use of consumer information solely to providing services to other businesses and financial institutions," and
- "[w]e limit sharing of non-public personal information to that necessary to complete the transactions on behalf of the consumer and the merchant and to that permitted by federal and state laws."

Id. at 593.

[282] *See, e.g., Beau Townsend Ford Lincoln Inc. v. Don Hinds Ford, Inc.*, Case No. 3:15-cv-400, 2017 WL 4237028 (S.D. Ohio Sept. 25, 2017) (holding that the buyer was liable to pay the seller $736,225.40 for 20 Ford Explorers, where the buyer had previously paid an internet hacker who pretended to be the seller's Sales Manager, using a Gmail account that appeared to belong to the Sales Manager, as a result of a security breach of the seller's email network, from which the scammer learned about the pending transaction and was able to spoof the seller's identity and send wire instructions that were acted upon by the buyer before the seller pursued payment, noting that "both parties were negligent in their business practices" because Beau Townsend Ford "should have maintained a more secure email system and taken quicker action upon learning that it might have been compromised" and Don Hinds Ford should have ascertained whether "an actual agent of Beau Townsend Ford was requesting that it send money by wire transfer.").

filed since 2010 over the alleged sharing of information with Internet advertisers and online behavioral advertising practices.[283] There may be several explanations for this. First, when a security breach occurs, cases brought by consumers often settle if there genuinely has been a loss (even if litigation with insurers and third parties over liability may continue). In consumer cases, the amount of individual losses may be limited both because security breaches do not always result in actual financial harm and because, when they do, federal law typically limits an individual consumer's risk of loss to $50 in the case of credit card fraud (and many credit card issuers often reimburse even that amount so that customers in fact incur no direct out of pocket costs). Class action settlements therefore may be focused on injunctive relief and *cy pres* awards, rather than large damage sums or may provide different settlement terms for those who experienced an actual financial loss compared to those who did not.[284] The propriety of *cy pres* awards was pending before

---

[283]*See supra* § 26.15 (analyzing data privacy putative class action suits).

[284]*See, e.g.*, *In re Target Corp. Customer Data Security Breach Litigation*, 892 F.3d 968 (8th Cir. 2018) (affirming final approval of a class action settlement, following remand, where Target agreed to pay $10 million to settle the claims of all class members and waived its right to appeal an award of attorney's fees less than or equal to $6.75 million. For those class members with documented proof of loss, the agreement called for full compensation of their actual losses up to $10,000 per claimant. For those class members with undocumented losses, the agreement directed a *pro rata* distribution of the amounts remaining after payments to documented-loss claimants and class representatives. Additionally, Target agreed to implement a number of data-security measures and to pay all class notice and administration expenses); *In re Anthem, Inc. Data Breach Litig.*, __ F.R.D. __, 2018 WL 3872788 (N.D. Cal. 2018) (granting final approval to a class action settlement of $115 million for a proposed class of approximately 79.15 million members with attorneys' fees capped at $37.95 million, in a suit for alleged negligence and breach of contract arising out of the Anthem Blue Cross security breach, after a cyberattack allegedly exposed insureds' personal data); *In re The Home Depot*, No. 14-MD-02583-TWT, 2017 WL 9605207 (N.D. Ga. Oct. 11, 2017) (awarding $15,300,000 in attorneys' fees, based on settlements of $27.25 million with consumers and $14.5 million with financial institutions, in a case arising out of a security breach); *In re the Home Depot, Inc*., Case No.: 1:14-md-02583-TWT, 2016 WL 6902351 (N.D. Ga. Aug. 23, 2016) (granting final approval of a $27.2 million settlement fund for a class of more than 52 million consumers in a suit arising out of a security breach); *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 851 F. Supp. 2d 1040 (S.D. Tex. 2012) (certifying a settlement class in a suit by credit cardhold-

the U.S. Supreme Court as this update went to press.[285] A ruling is expected by June 2019.

Second, because security breaches often revolve around a common event, where numerous cases are filed, they may be consolidated and transferred to a single district for pre-trial purposes by the Multi-District Litigation (MDL) panel.[286] By contrast, data privacy cases may involve similar alleged practices engaged in by multiple, unrelated companies or even entire industries, in somewhat different ways. Similar data privacy cases therefore typically have been brought as separate putative class action suits against different companies (or a single technology company and some of its customers, advertisers, or downstream recipients of data). A particular alleged practice therefore may spawn dozens of analogous lawsuits against different companies that do not end up being consolidated by the MDL Panel.

Third, in data privacy cases, publicity about some large settlements reached before the defendants even were served or answered the complaint drew attention and interest on the part of the class action bar that may have made those cases seem more appealing, at least initially.

In contrast to consumers, whose compensable injuries and risk of loss effectively are limited, commercial customers of companies that experience security breaches, such as the plaintiff in *Patco,* potentially bear the full risk of loss and are more motivated to sue (and have more substantial damage claims) than consumer plaintiffs. While breach cases where there has been an ascertainable, present loss may proceed, claims based merely on the potential risk of a future loss may or may not proceed past a motion to dismiss, depending on where suit is filed.

Some courts also have been more receptive to claims in security breach cases where real losses were experienced. For

---

ers against a transaction processor whose computer systems had been compromised by hackers, alleging breach of contract, negligence, misrepresentation and state consumer protection law violations, and approving a settlement that included *cy pres* payments totaling $998,075 to third party organizations and $606,192.50 in attorneys' fees).

[285] *See Frank v. Gaos,* 138 S. Ct. 1697 (2018) (granting *certiorari*).

[286] *See, e.g., In re Target Corp. Customer Data Security Breach Litig.*, 11 F. Supp. 3d 1338 (MDL 2014) (transferring to the District of Minnesota for coordinated or consolidated pretrial proceedings more than 33 separate actions pending in 18 districts and potential tag-along actions arising out of Target's 2013 security breach).

example, in *Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*,[287] the Fifth Circuit held that the economic loss doctrine did not bar issuer banks' negligence claims under New Jersey law and does not bar tort recovery in every case where the plaintiff suffers economic harm without any attendant physical harm where (1) plaintiffs, such as the Issuer Banks, constituted an "identifiable class," the defendant (in this case, Heartland) had reason to foresee that members of the identified class would be the entities to suffer economic losses were the defendant negligent, and the defendant would not be exposed to "boundless liability," but rather to the reasonable amount of loss from a limited number of entities; and (2) in the absence of a tort remedy, the plaintiffs, like the Issuer Banks in Heartland, would be left with no remedy at all for negligence, defying "notions of fairness, common sense and morality."

Contract limitations, while beneficial to companies in security breach litigation, may be more difficult to enforce against consumers. Marketing considerations may limit a company's ability to disclaim security obligations. Moreover, as a practical matter, it is unclear whether security obligations could ever be fully disclaimed in a consumer contract. The Federal Trade Commission has taken the position that a company's failure to maintain adequate security, even in the absence of affirmative representations, is an actionable violation of unfairness prong of section 5 of the Federal Trade Commission Act.[288] The FTC or state Attorneys General could bring enforcement actions or otherwise seek to apply pressure on a company that purported to disclaim obligations. Some security law obligations likewise may not be waived.

Since FTC Act violations are potentially actionable as violations of state unfair competition laws in some jurisdictions, a company's failure to adhere to implement reasonable security measures could be separately actionable regardless of what a company says about its practices. For example, California's notorious unfair competition statute, Cal. Bus. & Prof. Code § 17200, allows a private cause of action to be brought for violations of other statutes that do not expressly

---

[287] *Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013).

[288] *See supra* § 27.06.

create independent causes of action[289] (although only if the plaintiff has "suffered injury in fact and has lost money or property"[290] as a result of the violation).

While security breach class action suits may not be as lucrative for plaintiffs' counsel as some might have imagined—and even where a claim can be asserted a class may not be certified[291]—major security breaches have cost companies and their insurers substantial money.[292] Litigation involving risk of loss issues between companies and insurers, credit card companies, banks and merchants, and increasingly securities fraud class action suits, frequently involve higher dollar claims than consumer class actions arising out of a security breach.

As security law and practice evolves, the risks of litigation increase. FTC enforcement actions have encouraged the development of security-related best practices, including the adoption of information security programs. In addition, particular statutes, such as the Massachusetts law affirmatively mandating information security programs,[293] compel particular practices. Security breach notification statutes have created an even stronger incentive for businesses to address security concerns. Indeed, the requirement that companies notify consumers and in some cases state regulators of security breaches creates a tangible risk of litigation and regulatory enforcement actions—without any safe harbor to insulate businesses in the event a breach occurs despite best efforts to prevent one. Many of these statutes afford independent causes of action. Other state laws, such as California Bus. & Prof. Code § 1798.81.5—which compels businesses that own or license personal information about California residents to implement and maintain *reasonable* security procedures and practices appropriate to the nature of the information, to protect it from unauthorized access, destruc-

---

[289]*See, e.g., Kasky v. Nike, Inc.*, 27 Cal. 4th 939, 950, 119 Cal. Rptr. 2d 296 (2002); *Stop Youth Addiction, Inc. v. Lucky Stores, Inc.*, 17 Cal. 4th 553, 561–67, 71 Cal. Rptr. 2d 731, 736–40 (1998).

[290]Cal. Bus. & Prof. Code § 17200; *see generally supra* §§ 6.12[6], 25.04[3] (analyzing section 17200).

[291]*See, e.g.*, *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 293 F.R.D. 21 (D. Me. 2013) (denying plaintiffs' motion for class certification).

[292]Examples of the extent of liability incurred in connection with certain security breaches are set forth in section 27.01.

[293]*See supra* § 27.04[6][E].

tion, use, modification or disclosure—cannot be disclaimed and further invite potential litigation in the absence of any express definition of, or safe harbor for, what might be deemed *reasonable.*[294] Significantly, courts evaluating state law claims are not necessarily bound by the principle recognized by the FTC that "security breaches sometimes can happen when a company has taken every reasonable precaution."[295]

Without specific guidelines—such as those applied to financial institutions and covered health care entities under federal law—what constitutes adequate or reasonable conduct ultimately may present a fact question in litigation. The absence of safe harbors for businesses outside of the health care and financial services industries means that even businesses that implement the latest security technologies and industry "best practices" may be forced to defend themselves in litigation if a security breach occurs. As the cases discussed in this section illustrate, whether a claim for a breach is viable may depend on whether consumers are injured, which companies cannot easily control, and whether risk of loss provisions are addressed in contracts with vendors, banks, insurers and others, which a company may be able to influence, depending on its negotiating position and diligence in auditing its security-related agreements.

A company may limit its risk of litigation by entering into contracts with binding arbitration provisions and class action waivers, at least to the extent that there is privity of contract with the plaintiffs in any putative class action suit. While class action waivers are not universally enforceable as

---

[294] *But see Hutton v. National Board of Examiners in Optometry, Inc.*, 243 F. Supp. 3d 609, 613-15 (D. Md. 2017) (dismissing plaintiffs' claims under the California Customer Records Act, Cal. Civ. Code §§ 1798.81 *et seq.* and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, and for breach of contract, breach of implied contract, negligence and unjust enrichment, for lack of standing, where plaintiffs alleged that, as a result of a breach of a database containing PII from optometrists throughout the United States, they had incurred time and expenses (and, for one plaintiff, received a credit card that had not been requested, issued in the name she had used when she provided her PII to the defendant), because their assumption that the defendant suffered a data breach and was the source of the leaked data was based on online conversations, where plaintiffs "failed to allege a plausible, inferential link between the provision of PII to NBEO at some point in the past and their recent receipt of unsolicited credit cards.").

[295] *See* http://www.ftc.gov/opa/2003/11/cybersecurity.htm.

stand-alone agreements, a class action waiver that is part of a binding arbitration agreement is enforceable as a result of the U.S. Supreme Court's 2011 decision in *AT&T Mobility LLC v. Concepcion*.[296]

Even without a class action waiver, certification of a privacy or security breach class action generally will not be possible if the parties have entered into a binding arbitration agreement.[297] Arbitration provisions are broadly enforceable and, if structured properly, should insulate a company from class action litigation brought by any person with whom there is privity of contract.[298]

Where a claim is premised on an interactive computer service provider's republication of information, rather than direct action by the defendant itself, claims against the provider may be preempted by the Communications Decency Act.[299]

Additional, potentially relevant class action decisions are considered in section 26.15, which analyzes privacy-related class action suits.

---

[296]*AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011); *see generally supra* § 22.05[2][M] (analyzing the decision and more recent cases construing it and providing drafting tips for preparing a strong and enforceable arbitration provision); *see also supra* § 21.03 (online and mobile unilateral contract formation).

[297]*See, e.g., Meyer v. Uber Technologies, Inc.*, 868 F.3d 66 (2d Cir. 2017) (enforcing an online arbitration agreement where the company provided reasonable notice of the terms and the consumer manifested assent); *Tompkins v. 23andMe, Inc.*, 840 F.3d 1016, 1033 (9th Cir. 2016) (enforcing an arbitration provision in 23andMe's Terms of Service agreement as not unconscionable); *Pincaro v. Glassdoor, Inc.*, 16 Civ. 6870 (ER), 2017 WL 4046317 (S.D.N.Y. Sept. 12, 2017) (compelling arbitration of a putative security breach class action suit); *In re RealNetworks, Inc. Privacy Litig.,* Civil No. 00 C 1366, 2000 WL 631341 (N.D. Ill. May 8, 2000) (denying an intervenor's motion for class certification where the court found that RealNetworks had entered into a contract with putative class members that provided for binding arbitration); *see generally supra* § 22.05[2][M] (analyzing the issue and discussing more recent case law).

[298]*See supra* § 22.05[2][M][i] (analyzing *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011) and ways to maximize the enforceability of arbitration provisions).

[299]47 U.S.C.A. § 230(c); *supra* § 37.05.

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2019

Ian C. Ballon

NEW AND IMPORTANT FEATURES FOR 2019 NOT FOUND ELSEWHERE

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator — now a 5 volume set!

To order call **1-888-728-7677**
or visit **legalsolutions.thomsonreuters.com**

Key Features of E-Commerce & Internet Law

- The California Consumer Privacy Act, GDPR, California IoT security statute, Vermont data broker registration law, Ohio safe harbor statute and other important privacy and cybersecurity laws
- Understanding conflicting law on mobile contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- The most comprehensive analysis of the TCPA's application to text messaging and its impact on litigation found anywhere
- Complete analysis of the Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and Defend Trade Secrets Act (DTSA) and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, privacy obligations and the impact that Terms of Use and other internet and mobile contracts may have in limiting the broad exemption from liability otherwise available under CISA
- Comprehensive and comparative analysis of the platform liability of Internet, mobile and cloud site owners, and service providers, for user content and misconduct under state and federal law
- Understanding the laws governing SEO and SEM and their impact on e-commerce vendors, including major developments involving internet advertising and embedded and sponsored links
- AI, screen scraping and database protection
- Strategies for defending cybersecurity breach and data privacy class action suits
- Copyright and Lanham Act fair use, patentable subject matter, combating genericide, right of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of icons in mobile marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- How to enforce judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Compelling the disclosure of the identity of anonymous and pseudonymous tortfeasors and infringers
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions created by FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- Practical tips, checklists and forms that go beyond the typical legal treatise
- Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- Addresses both law and best practices
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

"Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet."
Jay Monahan
General Counsel, ResearchGate

****
ABOUT THE AUTHOR
****

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator based in the firm's Silicon Valley and Los Angeles offices. He defends data privacy, cybersecurity breach, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database and other intellectual property matters, including disputes involving Internet-related safe harbors and exemptions and platform liability.

Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top 75 Intellectual Property litigators, Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

In 2017 Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was named as the Lawyer of the Year for information technology law in the 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also serves as Executive Director of Stanford University Law School's Center for E-Commerce in Palo Alto.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

In addition to *E-Commerce and Internet Law: Treatise with Forms 2d edition*, Mr. Ballon is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Ed Chansky, Francoise Gilbert, Tucker McCrady, Josh Raskin, Tom Smedinghoff and Emilio Varanini.

NEW AND IMPORTANT FEATURES FOR 2019

- A comprehensive analysis of the **California Consumer Information Privacy Act**, **California's Internet of Things (IoT) security statute**, **Vermont's data broker registration law**, **Ohio's safe harbor** for companies with written information security programs, and other new state laws governing cybersecurity (chapter 27) and data privacy (chapter 26)
- An exhaustive analysis of **FOSTA-SESTA** and what companies should do to maximize CDA protection in light of these new laws (chapter 37)
- The **CLOUD Act** (chapter 50)
- Understanding **the TCPA after *ACA Int'l*** and significant new cases & circuit splits (chapter 29)
- Fully updated **50-state compendium** of security breach notification laws, with a **strategic approach** to handling notice to consumers and state agencies (chapter 27)
- **Platform liability and statutory exemptions and immunities** (including a comparison of "but for" liability under the CDA and DMCA, and the latest law on secondary trademark and patent liability) (chapter 49)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- The complex array of potential liability risks from, and remedies for, **screen scraping, database protection and use of AI to gather data and information online** (chapter 5)
- State online dating and revenge porn laws (chapter 51)
- **Circuit splits on Article III standing in cybersecurity litigation** (chapter 27)
- Revisiting **sponsored link, SEO and SEM practices and liability** (chapter 9)
- **Website and mobile accessibility** (chapter 48)
- **The Music Modernization Act's Impact on copyright preemption and DMCA protection for pre-1972 musical works** (chapter 4)
- **Compelling the disclosure of passwords and biometric information to unlock a mobile phone, tablet or storage device** (chapter 50)
- Cutting through the jargon to make sense of ***clickwrap*, *browsewrap*, *scrollwrap* and *sign-in wrap* agreements (and what many courts and lawyers get wrong about online contract formation)** (chapter 21)
- The latest case law, trends and strategy for **defending cybersecurity and data privacy class action suits** (chapters 25, 26, 27)
- **Click fraud** (chapter 28)
- Updated **Defend Trade Secrets Act** and UTSA case law (chapter 10)
- **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- **Applying the First Sale Doctrine to the sale of digital goods and information** (chapter 16)
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert) (chapter 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Music licensing** (updated by Tucker McCrady) (chapter 17)
- **Mobile, Internet and Social Media contests & promotions** (updated by Ed Chansky) (chapter 28)
- **Conducting a risk assessment and creating a Written Information Security Assessment Plan (WISP)** (by Thomas J. Smedinghoff) (chapter 27)