DEFENDING CYBERSECURITY BREACH CLASS ACTION LITIGATION

Excerpted from the latest update to Chapter 27
(Cybersecurity: Information, Network and Data Security)
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)
(These excerpts are unrevised page proofs for the current update and may contain errors)

INTERNET, AI & PRIVACY LAW YEAR IN REVIEW

MARCH 14, 2024

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:	Los Angeles:	Washington, D.C.:
1900 University Avenue, 5th Fl.	1840 Century Park East, Ste. 1900	2101 L Street, N.W., Ste. 1000
East Palo Alto, CA 914303	Los Angeles, CA 90067	Washington, D.C. 20037
Direct Dial: (650) 289-7881	Direct Dial: (310) 586-6575	Direct Dial: (202) 331-3138
Direct Fax: (650) 462-7881	Direct Fax: (310) 586-0575	Fax: (202) 331-3101

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

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
a 5-volume legal treatise by Ian C. Ballon
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, Facebook, Threads, BlueSky: 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
Suite 1900
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Washington, D.C.
2101 L Street, N.W.
Suite 1000
Washington, DC 20037
T 202.331.3138
F 202.331.3101

Ian C. Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, cybersecurity breach and AdTech class action suits.

Ian has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2024). He has been listed in Best Lawyers in America consistently every year since 2003 and was named Lawyer of the Year for Information Technology in 2024, 2023, 2022, 2020, 2019, 2018, 2016 and 2013. In 2024, 2023, 2022, 2021, 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In 2022, Ian was named to Lawdragon's list of the Top 500 Lawyers in America and he has been included on the *Daily Journal's* annual list of the Top 100 Lawyers in California. 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. He was also recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's Vanguard Award for significant contributions to the development of intellectual property law. Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named a Northern California Super Lawyer every year from 2004 through 2024 and a Southern California Super Lawyer for every year from 2007-2024. He has also been 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 and by Thomson Reuters as a Stand-Out Lawyer (in 2024) based on client nominations.

Ian is also the author of the leading treatise on internet and mobile law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. 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). In addition, he serves as Executive Director of Stanford University Law School's Center for the Digital Economy. He also chairs PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian holds JD and LLM degrees and the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 3

THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

higher level of oversight to ensure compliance.

27.07 Cybersecurity and Data Breach Litigation

27.07[1] In General

Litigation arising out of a data security breach may be brought by or against a business that suffered the attack. A company may choose to pursue civil or criminal remedies against the person(s) or entities responsible for the breach,[1] which in civil actions may require satellite litigation to compel the disclosure of the identity of an anonymous or pseudonymous thief.[2] A business that experienced a data loss also may be sued by its customers, users, or other third parties allegedly impacted by the breach, including in putative class action suits, which are addressed extensively in this section 27.07. 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

---

[Section 27.07[1]]

[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.

[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 allega-

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 laws that afford a statutory remedy for a security breach.[10] A business may also sue a vendor or other business partner responsible for a breach of its own systems, for negligence, breach of contract or similar claims, depending on the terms of their contract and the representations, warranties, and indemnifications provided, if any, and liability waivers.

Data security breaches may give rise to shareholder suits, including suits for securities fraud.[11] Security breach litigation also may arise between companies over responsibility

---

tion 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.

[10]*See infra* § 27.08[10][C].

[11]*See, e.g.*, *In re Alphabet, Inc. Securities Litigation*, 1 F.4th 687 (9th Cir. 2021) (affirming in part, reversing in part, the district court's dismissal of claims in a putative security breach class action suit alleging material misrepresentations in connection with Google's discovery of a security glitch in its Google+ social network, which had allegedly left the private data of users exposed to third-party developers for three years); *Reidinger v. Zendesk, Inc.*, Case No. 19-cv-06968-CRB, 2021 WL 796261 (N.D. Cal. Mar. 2, 2021) (dismissing a pension fund's securities fraud putative class action suit alleging "certain mistakes that resulted in a long-undetected breach"—for failing to plead a material misstatement or omission or scienter—because "although § 10(b) 'is aptly described as a catchall provision . . . what it catches must be fraud.' "; citing *Chiarella v. United States*, 445 U.S. 222, 235 (1980)); *In re Facebook, Inc. Securities Litigation*, 477 F. Supp. 3d 980 (N.D. Cal. 2020) (dismissing plaintiffs' amended complaint for lack of causation and reliance); *In re Facebook, Inc. Securities Litigation*, 405 F. Supp. 3d 809 (N.D. Cal. 2019) (dismissing plaintiffs' putative class action suit alleging that defendants made materially false and misleading statements and omissions concerning its privacy and data protection practices in violation of federal securities laws, where, among other things, statements anticipating the impact of new European privacy legislation on advertising revenues were "forward-looking statements" protected by Private Securities Litigation Reform Act's safe harbor

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 (and in credit card breach cases there may be parallel putative class action suits brought by financial institutions against merchants that experienced the breach, if it resulted in financial loss for the institutions).

Data breaches also have resulted in litigation with insurers over coverage issues. While many of these suits raise garden variety issues, litigation also has arisen over the more substantial question of whether the standard insurance exclusion for wars or military actions can be invoked to deny cyber insurance coverage for a malware attack originating with a state actor.[12]

Security breach suits brought by consumers against

---

provision, its CEO's conference call statement that he worked hard to make sure that the website complied with Facebook's FTC consent order was corporate puffery that was not actionable, and plaintiffs could not plead that Facebook's privacy policy statements were false); *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).

As in a consumer class action, causation in a securities fraud case may be difficult to establish. Thus far, it has proven challenging for plaintiffs to present an accurate measure of loss tied to a cybersecurity incident.

[12]An insurer typically excludes acts of war from coverage out of concern that global events affecting large numbers of insureds could bankrupt the insurer. When governments place blame for cybersecurity incidents on state actors, they potentially deprive affected businesses of insurance coverage, depending on the language of applicable policies. Some policies, however, include cyberterrorism protection, as an express exception to the exclusion for acts of war.

Mondelez International, Inc. sued Zurich American Insurance Company over Zurich's invocation of the "hostile or war like" exclusion clause in Mondelez's $100 million cyber insurance policy, after 1,700 servers and 24,000 Mondelez laptops allegedly were rendered "permanently dysfunctional" by the NotPetya malware attack, which the U.S., U.K. and a number of other governments identified as a Russian government attack, targeted at Ukraine. *See Mondelez Int'l, Inc. v. Zurich American Insurance Co.*, Case No. 2018LO11008 (Cook Co. Ill. Cir. Court Complaint filed Oct. 10, 2018); Oliver Ralph and Robert Armstrong, *Mondelez sues Zurich in test for cyber hack insurance*, Financial Times, Jan. 9, 2019. NotPetya was a ransomware attack that was first detected in Ukraine on June 27, 2017, and spread throughout the world quickly. *See generally*

companies that have experienced a breach frequently are framed in terms of common law and state statutory remedies. The most common theories of recovery are breach of contract, breach of implied contract (if there was no express contract), breach of fiduciary duty, public disclosure of private facts, and negligence, depending on the facts of a given case. There is no single federal statute providing a cause of action for a cybersecurity breach impacting consumers.

Those few federal statutes that impose express data security obligations on persons and entities—The Children's Online Privacy Protection Act[13] (which regulates information collected from children under age 13), The Gramm-Leach-Bliley Act (which imposes security obligations on financial institutions[14]) and the Health Insurance Portability and Accountability Act (HIPAA)[15] (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). Depending on the facts alleged, claims also sometimes may be asserted under federal computer crime statutes, such as the Stored Communications Act,[16] but those statutes usually are not well-suited to data breach cases.[17] Claims arising out of security breaches

---

Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, Aug. 8, 2018; Brian Corcoran, *What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict*, https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict (posted Mar. 8, 2019).

[13]15 U.S.C.A. §§ 6501 to 6506; *supra* §§ 26.13[2], 27.04[2].

[14]15 U.S.C.A. §§ 6801 to 6809, 6821 to 6827; *supra* § 27.04[3].

[15]42 U.S.C.A. §§ 1320d *et seq.*; *supra* § 27.04[4].

[16]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).

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

also have been brought under the Fair Credit Reporting Act,[18] but that statute imposes obligations on consumer reporting agencies, users of consumer reports, and furnishers of information to consumer reporting agencies,[19] 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.[20]

---

formation 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.

[18]15 U.S.C.A. §§ 1681 *et seq.*

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

[20]*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 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

Class action lawyers also 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.[21] If 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.[22] Public companies that experience data breaches also may be subject to securities fraud class action suits.[23]

Suits brought by California residents for cybersecurity breaches under the California Consumer Privacy Act[24] (and how the nature of that litigation will change with the planned implementation of the California Privacy Rights Act (CPRA)) are separately analyzed in section 26.13A[14].

A company's obligation to comply with security breach notification laws may result in publicity that leads to consumer litigation, including class action litigation, as well as regulatory scrutiny (which, if it proceeds to the point where an enforcement action is publicly disclosed, also may lead to putative class action litigation).[25]

Higher stakes security breach litigation typically is

---

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").

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

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

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

[24]Cal. Civ. Code § 1798.150(a)(1); *see generally supra* § 26.13A[14] (analyzing CCPA and CPRA security breach litigation).

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

brought by business customers of a company that has experienced a breach over which party bears the risk of loss (if substantial losses were incurred). By contrast, consumers often are insulated from the financial consequences of a security breach so damage claims may be more modest in consumer litigation (absent the availability of statutory damages), although the number of potential claimants may be greater.

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).[26] 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 in federal court or to 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),[27] breach of fiduciary duty, negligence or similar claims, depending on the facts of

---

[26]*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).

[27]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 enforce-

a given case.[28] These common law claims rarely afford either statutory damages or attorneys' fees, however, so plaintiffs 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 Article III standing to even maintain suit.[29] While there typically is not the same standing requirement to sue in state court (which are

---

ability of the Privacy Pledge under a plethora of state laws weighs strongly against a finding of commonality."); *see generally supra* §§ 26.14 (privacy policies), 26.15 (privacy litigation).

[28]*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 making 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). *But see In re SuperValu, Inc., Customer Data Security Breach Litig.*, 925 F.3d 955 (8th Cir. 2019) (affirming dismissal of all claims following remand).

[29]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 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); *see also Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020) ("To establish standing under Article III of the Constitution, a plaintiff must demonstrate (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief.").

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,* 570 U.S. 693, 695-96 (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).

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 cases most directly relevant to future harm are *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), and an earlier case, *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), in which the Supreme Court made clear that allegations of "possible future injury" are not sufficient. 568 U.S. 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 *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), the Supreme Court tightened the requirements for standing in cases involving statutory violations and the threat of future harm, holding that while the material risk of future harm may satisfy the concrete-harm requirement in connection with a claim for injunctive relief in appropriate cases, the mere risk of future harm, without more, is insufficient to establish concrete

harm to justify standing when damages are sought. In *Ramirez*, TransUnion offered customers an OFAC Name Screen Alert, which identified users whose names were included on a list maintained by the U.S. Treasury Department's Office of Foreign Assets Control of suspected terrorists, drug traffickers and other serious criminals. *Ramirez* involved a certified class of 8,185 individuals who had OFAC alerts in their credit files and alleged that TransUnion violated the Fair Credit Reporting Act by failing to use reasonable procedures to ensure the accuracy of their credit files. The Court held that 1,853 class members, including Ramirez, who had had the OFAC information communicated to third parties, had suffered a harm with a "close relationship" to the harm associated with the tort of defamation and therefore had Article III standing. By contrast, the remaining 6,332 class members whose files also contained misleading OFAC alerts did not have standing because the information was not communicated to any third party and "the mere existence of inaccurate information in a database is insufficient [absent dissemination] to confer Article III standing." *Id.* at *11. The Court also held that formatting errors in the notices sent to all class members did not justify standing because plaintiffs did not demonstrate that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts under *Spokeo*. *See infra* § 27.07[2][B] (analyzing *Ramirez* and its impact on cybersecurity class action litigation).

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.").

With respect to redressability, the Supreme Court has held that nominal damages may satisfy this requirement. *See Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 797-802 (2021) (holding that "a request for nominal damages satisfies the redressability element of standing where a plaintiff's claim is based on a completed violation of a legal right."). Justice Thomas, for the majority in *Uzuegbunam*, wrote:

> At all stages of litigation, a plaintiff must maintain a personal interest in the dispute. The doctrine of standing generally assesses whether that interest exists at the outset, while the doctrine of mootness considers whether it exists throughout the proceedings. To demonstrate standing, the plaintiff must not only establish an injury that is fairly traceable to the challenged conduct but must also seek a remedy that redresses that injury. And if in the course of litigation a court finds that it can no longer provide a plaintiff with any effectual

courts of general jurisdiction),[30] class action lawyers often prefer to be in federal court to seek certification of potentially larger national class actions. Even if plaintiffs have not been injured and have no recoverable damages, the potential cost of defending a class action and potential adverse publicity[31] encourage some defendants to settle—and the larger the class, the greater the value of a potential settlement in the eyes of some plaintiffs' counsel. Other defendants fight, attacking the pleadings on a motion to dismiss, and presenting evidence in support of summary judgment (and potentially moving to exclude experts, pursuant to *Daubert* motions[32]). If a case progresses, the parties typically will engage in discovery in advance of any motion for class certification. Where discovery occurs, businesses may want to shield their proprietary systems and information through use of a protective order.[33]

---

relief, the case generally is moot. This case asks whether an award of nominal damages by itself can redress a past injury. We hold that it can.

Id. at 796.

[30]A small number of state courts may apply similar standing requirements. *See, e.g.*, *Abernathy v. Brandywine Urology Consultants, P.A.*, C.A. No. N20C-05-057 MMJ CCLD, 2021 WL 211144, at *2-6 (Del. Sup. Jan. 21, 2021) (dismissing a suit brought by plaintiff-patients, holding that they lacked standing in suit brought over a malware attack that blocked access to defendant's computer system and data, which included sensitive patient medical records, when cyberthieves accessed and encrypted records that included patient names, addresses, Social Security numbers, medical file numbers, claim data, and other financial and personal data but never sought to extract a ransom; "While the complaint provides information about medical disruption in the abstract, it fails to identify even one plaintiff who was denied access to their medical records or had their medical treatment otherwise disrupted."). State courts also may impose dollar value minimum or maximum thresholds for jurisdictional purposes. Otherwise, however, a plaintiff generally need not establish standing in state court (other than statutory standing for suits brought under statutes that create statutory standing requirements), although the absence of damage or injury may provide grounds for a motion to dismiss or demurrer under applicable state court practice or otherwise preclude a plaintiff from prevailing on the merits.

[31]Potential concerns about adverse publicity have become less significant as virtually every company and every consumer in America has been the victim of a security breach (if not multiple breaches).

[32]*See, e.g.*, *In re Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 16-MD-02752-LHK, 2020 WL 4212811, at *9 (N.D. Cal. July 22, 2020) (discussing efforts to exclude experts in connection with approving a class action settlement).

[33]*See infra* § 27.07[5] (addressing confidentiality, privilege and protec-

Plaintiffs' counsel also increasingly seek to challenge privilege designations in connection with forensic investigations into security incidents, which is addressed in section 27.07[5].

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, putative consumer data breach class action suits may raise complicated issues associated with proving causation[34]—especially where a given consumer has had his or her information compromised more than one time[35] or

---

tive orders in data breach litigation).

[34]*See, e.g.*, *Galaria v. Nationwide Mutual Insurance Co.,* Case No. 2:13-cv-118, Case No. 2:13-cv-257, 2017 WL 4987663, at *6-7 (S.D. Ohio Aug. 16, 2017) (denying leave to file an amended complaint repleading negligence based on futility, where plaintiffs alleged that a data breach occurred and that, fifteen months later, three unsuccessful attempts were made to open credit cards in one plaintiff's name using information that may have been available as a result of the data breach, because plaintiffs could not establish causation; "At best, Plaintiffs have alleged nothing more than time and sequence. Given the lengthy time gap of well over a year between the data breach and the alleged unauthorized attempts to open credit cards, that is far from sufficient to suggest that the misuse of Mr. Galaria's personal information plausibly resulted from that breach."); *Fu v. Wells Fargo Home Mortgage*, Civil Action No. 2:13–cv–01271–AKK, 2014 WL 4681543, at *4-5 (N.D. Ala. Sept. 12, 2014) (granting summary judgment for the defendant on plaintiff's negligence claim for lack of causation where identity theft had "multiple possible causes" yet plaintiff failed to "provide[] sufficient evidence . . . that the unsecured email led to the [identity] theft," as opposed to "other possible theories" including that the thief "obtained [plaintiff's] personal information from sources other than the email"); *Jones v. Commerce Bank, N.A.*, No. 06 Civ. 835(HB), 2007 WL 672091, at *4 (S.D.N.Y. Mar. 6, 2007) (granting summary judgment for the defendant on plaintiff's negligence claim based on identity theft because "[t]he thieves might well have stolen Plaintiff's information without any negligence on the part of [defendant]"); *see also In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1035-38 (N.D. Cal. 2021) (dismissing plaintiffs' California invasion of privacy claim, in a putative class action suit, where plaintiffs failed to allege "that Zoom actually shared *their* personal data with third parties.") (emphasis in original); *see generally infra* § 27.07[3] (analyzing causation, proof of injury, and damages in cybersecurity breach putative class action suits).

[35]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.

where a company incurred a loss despite taking industry standard precautions to prevent a breach. Finally, even where liability, including causation, may be established, if there has been no harm, damages may be merely speculative.[36] 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 July 2021, no data security breach class action suit brought by a class of consumers had 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). Class action settlements are addressed in section 27.07[6].

Cybersecurity breach litigation under the California Consumer Privacy Act (CCPA) is separately analyzed in section 26.13A[14] in chapter 26.

The following subsections address Article III standing (in general, in section 27.07[2][A], and in greater detail, and in chronological order so as to better understand the evolution of Supreme Court doctrine, current circuit splits, and what cases remain good law (and in which circuits), in section 27.07[2][B]), elements of claims (including causation and proof of harm) and class certification (in section 27.07[3]), MDL consolidation in cybersecurity putative class action suits (in section 27.07[4]), preservation of privilege and confidentiality in putative data breach class action litigation (in section 27.07[5]), and settlement data and procedural issues (in section 27.07[6]). Business to business litigation, future trends, arbitration and other class action litigation issues in data breach cases are addressed in subsection 27.07[7]. Class certification issues are addressed more extensively in section 25.07[2] in chapter 25.

---

[36] *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962–63 (S.D. Cal. 2012) ("[t]he breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action for negligence.").

27.07[2] Article III Standing in Data Breach Cases

27.07[2][A] Article III Standing in Cybersecurity Data Breach Putative Class Action Litigation—In General

A threshold question in most security breach putative class action suits filed in federal court is whether the plaintiffs have standing to maintain suit. Standing initially must be established based on the named plaintiffs that actually filed suit, not unnamed putative class members.[1] If a class ultimately is certified, however, every class member must have standing.[2]

Standing may be addressed at any time, but frequently is raised at the outset of a case (or in response to an amended Complaint) pursuant to Federal Rule of Civil Procedure 12(b)(1) (for lack of subject matter jurisdiction) based plaintiff's allegations and potentially (but not necessarily) supported by declarations or other evidence submitted in support of the motion by the defendant.

Where a plaintiff in fact has incurred financial harm or was the victim of identity theft, standing generally will be

---

[Section 27.07[2][A]]

[1]*See, e.g.*, *Simon v. Eastern Kentucky 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) ("Standing cannot be acquired through the back door of a class action." (internal quotation omitted)); *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).

[2]*See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021) (holding that while the named plaintiff and 1,853 class members who prevailed at trial in a Fair Credit Reporting Act suit had standing, the other 6,332 class members (whose incorrect credit report information was not provided to third parties) did not have standing), *rev'g,* 951 F.3d 1008, 1023 (9th Cir. 2020).

established.[3] In most data breach cases, however, information may have been exposed but the plaintiff has not incurred any present economic harm and therefore sues based on the potential threat of future injury and/or the costs and time incurred to mitigate that potential risk.

The ability of plaintiffs to establish Article III standing in such cases has been circumscribed by a trio of U.S. Supreme Court cases—*Clapper v. Amnesty Int'l USA*[4] (which addressed standing based on the threat of future injury in a case seeking injunctive relief), *Spokeo, Inc. v. Robins*[5] (which set out the parameters for establishing standing where a plaintiff can state a claim under a federal statute that doesn't otherwise require a showing of injury, and was a compromise opinion by eight justices following the untimely death of Justice Scalia) and *TransUnion LLC v. Ramirez*,[6] in which a more conservative court, with three new Trump appointees who had not been members of the Court that decided *Spokeo,* further tightened the standards for establishing Article III standing based on the threat of future harm, limited *Clapper* to cases involving injunctive relief, and held that the risk of future harm, without more, does not justify standing.

Although plaintiffs' counsel often 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

---

[3]*See, e.g.*, *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); *Hapka v. Carecentrix, Inc.*, Case No. 16-2372-CM, 2016 WL 7336407, at *2-4 (D. Kan. Dec. 19, 2016) (finding standing in a security breach case where the plaintiff alleged that she was the victim of tax fraud as a consequence of the breach).

[4]*Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409-11 (2013) (reiterating 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, and holding that to establish standing, a future injury must be "certainly impending," rather than speculative or based on "a highly attenuated chain of possibilities . . . .").

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

[6]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021).

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.[7] Further, as clarified by the U.S. Supreme Court in *TransUnion LLC v. Ramirez*[8] in 2021, a material risk of future harm can satisfy the concrete-harm requirement in the context of a claim for injunctive relief to prevent harm from occurring, if the harm is sufficiently imminent and substantial, but the mere risk of future harm cannot qualify as a concrete harm in a suit for damages (at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm).[9]

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 where a plaintiff has had personal information exposed but not incurred any economic harm or been subject to identity theft or other fraudulent misconduct as a result of the data breach. The Seventh,[10] Ninth,[11] and D.C. Circuits,[12] as well as the

---

[7] *Susan B. Anthony List v. Driehaus,* 573 U.S. 149, 157-58 (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).

[8] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

[9] *See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210-11 (2021) (emphasis in original).

[10] *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 *Remijas* 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).

[11] *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), *cert. denied*, 139 S. Ct. 1373 (2019).

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 within the Ninth Circuit 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 "*Clap-*

Sixth Circuit[13] in a non-precedential opinion, and district courts elsewhere,[14] apply a very liberal standard in evaluating assertions of standing based on future harm, which makes it easier for plaintiffs to establish standing in data

---

per 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); *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).

[12]*See In re U.S. Office of Personnel Management Data Security Breach Litig.*, 928 F.3d 42, 54-61 (D.C. Cir. 2019) (following *Attias* in finding standing in a multi-month cyberattack involving the theft of the personnel records of 21.5 million government employees, over the objection of the dissent that with the passage of time it was not plausible that this attack was undertaken to commit identity theft, and more plausibly involved foreign espionage); *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).

[13]*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").

[14]*See, e.g.*, *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231 (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).

breach cases in those circuits based merely on the potential future risk of financial harm or identity theft. The liberal approach is more difficult to reconcile with Supreme Court precedents—especially after *TransUnion LLC v. Ramirez*.[15]

By contrast, the Fourth,[16] Eighth[17] and Eleventh[18] Circuits,

---

[15]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021). *Ramirez* is analyzed in section 27.07[2][B].

[16]*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.*, 892 F.3d 613 (4th Cir. 2018) (finding standing where plaintiffs had had Chase Amazon Visa credit card accounts opened in their names (or maiden names) without their knowledge or approval, which they alleged to be traceable to the National Board of Examiners, which they believed to be the only common source to which they (and other optometrists in whose names fraudulent Chase Amazon Visa credit card accounts had been established) had given personal information, even though they had not alleged that they had incurred fraudulent charges (merely the costs for mitigating measures to safeguard against future identity theft), because the injuries alleged were not speculative—plaintiffs had shown a substantial risk of harm based on the fraudulent credit card accounts; "although incurring costs for mitigating measures to safeguard against future identity theft may not constitute an injury-in-fact when that injury is speculative, . . . the Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists . . . .").

[17]*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); *see also In re SuperValu, Inc., Customer Data Security Breach Litig.*, 925 F.3d 955 (8th Cir. 2019) (affirming dismissal, for failure to state a claim, of all claims following remand).

[18]*See Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1340-45 (11th Cir. 2021) (affirming dismissal of plaintiff's breach of implied contract, negligence, unjust enrichment, unfair competition and related claims, arising out of the data breach of a restaurant's point of sale system, which allegedly exposed plaintiff's (and other customers') credit card and other financial information, and as a result of which plaintiff alleged three types of injuries suffered in his efforts to mitigate the perceived risk of future identity theft: lost cash back or reward points (due to lost use from canceling and waiting for reissued credit cards), lost time spent addressing the problems caused by the cyber-attack, and restricted card access resulting from his credit card cancellations).

as well as arguably the Second Circuit,[19] apply a more exacting standard that is more consistent with the most recent U.S. Supreme Court case law on standing, as do the First[20] and Third[21] Circuits in older opinions that pre-date *Clapper*.

---

[19]*See McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 299-305 (2d Cir. 2021) (holding that a plaintiff may establish standing based on an "increased risk" theory of Article III standing in appropriate circumstances, but affirming dismissal of plaintiff's suit for lack of standing where the defendant accidently sent an email to all of its approximately 65 employees attaching a spreadsheet containing sensitive PII (including Social Security numbers, home addresses, birth dates, phone numbers, educational degrees, and dates of hire) of approximately 130 then-current and former employees, where plaintiffs failed to allege that their PII was subject to a targeted data breach or allege any facts suggesting that their PII (or that of any other similarly situated people) was misused, and hence failed to allege that they were at a substantial risk of future identity theft or fraud sufficient to establish Article III standing); *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).

[20]*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").

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

Reilly has been applied post-*Clapper* in numerous district court opinions in the Third Circuit. *See, e.g.*, *Browne v. US Fertility LLC,* Civil Action No. 21-367, 2021 WL 2550643, at *2-3 (E.D. Pa. June 22, 2021) (following *Reilly* in dismissing plaintiff's putative class action suit arising out of the theft of patient personal information from Shady Grove Fertility

clinics in Pennsylvania, Maryland, and New Jersey, holding that Browne's expenditure of $181.27 to purchase LifeLock services did not establish injury-in-fact and that he could "not achieve standing on the allegation that Defendants breached an implied contract or were unjustly enriched."); *Graham v. Universal Health Service, Inc.*, Civil Action No. 20-5375, 2021 WL 1962865, at *3-5 (E.D. Pa. May 17, 2021) (dismissing plaintiffs' putative class claims, arising out of a ransomware attack, for those plaintiffs whose injuries were premised on future risks and preventative measures, while denying defendant's motion to dismiss brought by the one plaintiff who alleged that his insurance premiums were increased as a result of the attack; "The target of a ransomware attack is the holder of the confidential data; the misappropriation of the data, whether by theft or merely limitation on access to it, is generally the means to an end: extorting payment. A court is still left to speculate, as in *Reilly*, whether the hackers acquired Plaintiffs' PHI in a form that would allow them to make unauthorized transactions in their names, as well as whether Plaintiffs are also intended targets of the hackers' future criminal acts."); *Clemens v. ExecuPharm, Inc.*, Civil Action No. 20-3383, 2021 WL 735728, at *3-5 (E.D. Pa. Feb. 25, 2021) (following *Reilly* in dismissing plaintiff's claims arising out of a ransomware attack undertaken by CLOP, for lack of standing, where plaintiff, a former employee, had her information (including her Social Security number, banking information (a copy of a personal check for direct deposit), driver's license, date of birth, home address, spouse's name, beneficiary information (including Social Security numbers) and payroll tax forms (such as W-2 and W-4)) stolen and released on the dark web, which she had argued evidenced that harm was certainly impending, despite alleging that she experienced actual harm from her time, money and effort to protect her information based on the imminent risks she allegedly faced, and that she alleged harm to her private contract rights); *In re Rutter's Inc. Data Security Breach Litigation*, 511 F. Supp. 3d 514 (M.D. Pa. 2021) (applying *Reilly* in holding that plaintiffs could not establish standing where their credit card information had been exposed but they had not incurred any loss; "As in *Reilly*, the harm that Plaintiffs . . . may face in the future—even if that harm is arguably more likely to occur than in *Reilly*—depends on multiple levels of impermissible speculation. To hold here that a plaintiff in a data breach class action, who has presently suffered no cognizable injury, can establish standing with allegations that she suffers some unquantifiable risk of future harm based on the lone fact that other people were harmed would totally undermine *Reilly*'s bright-line rule."); *Storm v. Paytime, Inc*., 90 F. Supp. 3d 359, 364-68 (M.D. Pa. 2015) (applying *Reilly* in holding that employees lacked standing to sue over a cyber-attack that had occurred a year earlier but not resulted in any actual misuse of data, and that incurring costs to take certain precautions following the breach was not an injury in fact, and that the attack did not establish standing invasion of a privacy right; "the Third Circuit requires its district courts to dismiss data breach cases for lack of standing unless plaintiffs allege actual misuse of the hacked data or specifically allege how such misuse is certainly impending. Allegations of increased risk of identity theft are insufficient to allege a harm. . . . Plaintiffs argue that the different verbs used in their allegations, such as 'stolen' and 'misappropriated,' distinguish their case from *Reilly* in such a way as

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 Article III standing.

Some courts have suggested that there isn't really a circuit split on the issue of the level of harm required to establish Article III standing in a security breach case premised on the threat of future harm, and that "the differing sets of facts involved in each circuit's decision are what appear to have driven the ultimate decision on standing, not necessarily a fundamental disagreement on the law."[22] According to this view, courts should look to (1) the motive of the hacker,

---

to create a cognizable harm, but this is a strained argument, which would require the Court to ignore the substance of the allegations. . . . [F]or a court to require companies to pay damages to thousands of customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to businesses. There is simply no compensable injury yet, and courts cannot be in the business of prognosticating whether a particular hacker was sophisticated or malicious enough to both be able to successfully read and manipulate the data and engage in identity theft.").

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.' "); *see also Gennock v. Kirkland's Inc.*, No. 17-454, 2017 WL 6883933, at *5 (W.D. Pa. Nov. 29, 2017) (distinguishing between *Horizon* and *Reilly* "on the basis that [*Reilly*] involved common law claims, whereas in *Horizon* the plaintiffs cited an act in which Congress elevated the unauthorized disclosure of information into a tort").

[22] *In re 21st Century Oncology Customer Data Security Breach Litigation*, 380 F. Supp. 3d 1243, 1251 (M.D. Fla. 2019); *see also, e.g.*, *McMorris v. Carlos Lopez & Associates, LLC,* 995 F.3d 295, 299-305 (2d Cir. 2021) (seeking to harmonize divergent circuit court views, while not addressing specifically *21st Century Oncology*; "in actuality, no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft—even those courts that have declined to find standing on the facts of a particular case."); *Finesse Express, LLC v. Total Quality Logistics, LLC*, Case No. 1:20cv235, 2021 WL 1192521, at *3 (S.D. Ohio

to the extent discernable; (2) the type of information compromised, including whether it is "easily changeable or replaceable information, such as credit and debit card information, and personally identifiable information, such as social security numbers, birth dates, or driver's license numbers, which is more static;" and (3) whether "there is evidence that a third-party has accessed the sensitive information and/or already used the compromised data fraudulently."[23] Relatedly, the Second Circuit sought to harmonize divergent rulings by suggesting that its sister circuits (at least prior to *TransUnion LLC v. Ramirez*[24]) reached the outcomes they did depending on whether: (1) the data at issue had been compromised as the result of a targeted attack intended to obtain the plaintiffs' data; (2) at least some part of the compromised dataset had been misused—even if plaintiffs' particular data (subject to the same security incident) had not been (or not yet been) affected; and (3) the type of data at issue was more or less likely to subject plaintiffs to a perpetual risk of identity theft

---

Mar. 31, 2021) (quoting *21st Century Oncology* on this point); *Portier v. NEO Technology Solutions*, Case No. 3:17-cv-30111, 2019 WL 7946103, at *7-8 (D. Mass. Dec. 31, 2019) (applying *21st Century Oncology*), *report and recommendation adopted*, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *In re Brinker Data Incident Litigation*, Case No. 3:18-cv-686-J-32MCR, 2019 WL 3502993, at *6 (M.D. Fla. Aug. 1, 2019) (applying *21st Century Oncology*). *But see, e.g.*, *Blahous v. Sarrell Regional Dental Center for Public Health, Inc.*, Case No. 2:19-cv-798-RAH-SMD, 2020 WL 4016246, at *5 (M.D. Ala. July 16, 2020) (disagreeing with *21st Century Oncology*; "In applying this standing jurisprudence to data breach cases, the vast majority of federal courts have reached the same conclusion despite differing interpretations of the Supreme Court's decision in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). . . . Bound by *Clapper*'s logic, lower federal courts presented with 'lost data' or potential identity theft cases in which there is no proof of *actual* misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data.").

[23] *Finesse Express, LLC v. Total Quality Logistics, LLC*, Case No. 1:20cv235, 2021 WL 1192521, at *3 (S.D. Ohio Mar. 31, 2021) (finding standing to assert claims for negligence, breach of contract, unjust enrichment, and declaratory and injunctive relief); *In re 21st Century Oncology Customer Data Security Breach Litigation*, 380 F. Supp. 3d 1243, 1251-54 (M.D. Fla. 2019); *see also, e.g.*, *Portier v. NEO Technology Solutions*, Case No. 3:17-cv-30111, 2019 WL 7946103, at *7-8 (D. Mass. Dec. 31, 2019), *report and recommendation adopted*, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *In re Brinker Data Incident Litigation*, Case No. 3:18-cv-686-J-32MCR, 2019 WL 3502993, at *6 (M.D. Fla. Aug. 1, 2019).

[24] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021); *see generally infra* § 27.07[2][B].

or fraud once it had been exposed.[25]

While factual differences certainly make a difference in standing determinations, a close analysis of circuit court case law, and how it evolved, reveals sharp differences in the approaches of at least a number of the federal circuit courts.[26]

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, the following section (section 27.07[2][B]) 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*[27] (which tightened the standards for standing based on the threat of future injury), *Spokeo, Inc. v. Robins*[28] (which addressed standing in cases where a plaintiff is able to state a claim under a federal statute that doesn't otherwise require a showing of injury), and

---

[25]*See McMorris v. Carlos Lopez & Associates, LLC,* 995 F.3d 295, 301-02 (2d Cir. 2021). The Second Circuit cautioned that:

> These factors are by no means the only ones relevant to determining whether plaintiffs have shown an injury in fact based on an increased risk of future identity theft or fraud. After all, determining standing is an inherently fact-specific inquiry that "requires careful judicial examination of a complaint's allegations to ascertain whether the particular plaintiff is entitled to an adjudication of the particular claims asserted." *Allen v. Wright*, 468 U.S. 737, 752 (1984). Nevertheless, these are the considerations that our sister circuits have most consistently addressed in the context of data breaches and other data exposure incidents, and we agree that they provide helpful guidance in assessing whether plaintiffs have adequately alleged an injury in fact."

Id. at 302-03. Nonetheless, the *McMorris* panel also observed that "in actuality, no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft—even those courts that have declined to find standing on the facts of a particular case." *Id.* at 299; *see generally infra* § 27.07[2][B] (analyzing *McMorris* and the other leading circuit court opinions in greater detail, in chronological context, and in light of *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021)).

[26]*See infra* § 27.07[2][B].

[27]*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 410.

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

TransUnion LLC v. Ramirez,[29] in which a more conservative court, with three new Trump appointees who were not members of the Court that decided *Spokeo,* further tightened the standards for establishing standing based on the threat of future harm, limited *Clapper* to cases involving injunctive relief, and held that the risk of future harm, without more, does not justify Article III standing.

It is also helpful to understand the procedural posture of a case when standing is raised.[30] A defendant may challenge subject-matter jurisdiction in one of two ways: facially or factually.[31] At the pleading stage, injury may be shown by "general factual allegations of injury resulting from the defendant's conduct."[32] The appropriate standard is akin to one of general, rather than proximate causation.[33] 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 . . . ."[34] Nevertheless, the requirement, even at the pleading stage, has been clarified

---

[29]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021).

[30]*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,* 137 S. Ct. 2307 (2017).

[31]*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). Where a defendant challenges standing based solely on the allegations of plaintiff's Complaint, a court will assume as true all material allegations and generally will construe the Complaint in favor of the complaining party. *E.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 597 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1684 (2021).

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

[33]*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.,* 572 U.S. 118, 134 n.6 (2014) ("Proximate causation is not a requirement of Article III standing.")).

[34]*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.

to require a plaintiff to " 'clearly allege facts' demonstrating" the elements of standing.[35] The plaintiff must allege a basis for standing that is *plausible*.[36]

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."[37] "In this posture, 'the presumption of truthfulness normally accorded a complaint's allegations does not apply.' "[38]

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.[39] A number of courts, however, have rejected the notion that credit monitoring

---

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).

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

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

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

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

[39]For this reason, companies that experience a security breach sometimes voluntarily offer affected consumers free credit monitoring services—even in breaches where the information exposed could not lead to identity theft or credit card fraud—to deprive plaintiffs' counsel of a potential argument for standing to sue in litigation in federal court. *See*

costs (or similar expenses incurred to mitigate a potential future harm) can confer standing where the threat that these costs address is itself viewed as speculative or at least not certainly impending.[40] As the U.S. Supreme Court explained

---

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.*

[40]*See, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011), *cert. denied*, 566 U.S. 989 (2012); *Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) ("although incurring costs for mitigating measures to safeguard against future identity theft may not constitute an injury-in-fact when that injury is speculative, . . . the Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists . . . ."); *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."); *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1344-45 (11th Cir. 2021) (rejecting mitigation efforts Tsao ostensibly took following notice of the breach, when he notified Wells Fargo and Chase to cancel his credit cards and allegedly suffered three distinct injuries: (1) lost opportunity to accrue cash back or rewards points on his cancelled credit cards, (2) costs associated with detection and prevention of identity theft in taking the time and effort to cancel and replace his credit cards; and (3) restricted account access to his preferred payment cards); *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); *see also McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 303 (2d Cir. 2021) ("this case presents a related question of standing: where plaintiffs take steps to protect themselves following an unauthorized data disclosure, can the cost of those proactive measures alone constitute an injury in fact? We agree with the district court that the answer is "no." . . . That is, where plaintiffs have shown a substantial risk of future identity theft or fraud, 'any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact.' . . . But where 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.' "). 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

in *Clapper v. Amnesty International USA*,[41] plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[42] 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.[43] In a subsequent Seventh Circuit case, the court even found 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

---

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, and which held that Neiman Marcus' offer of free credit monitoring was evidence that plaintiffs faced a concrete risk of harm and therefore justified standing in that case. *Moyer* continues to be cited on other grounds, however, and Judge Bucklo's analysis of Clapper appears justified in light of the Supreme Court's subsequent opinion in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

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

[42] *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.

[43] *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 *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).

defendant's security breach.[44] 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.[45]

While credit monitoring alternatively has been seen as a 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

---

[44]*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).

[45]Connecticut, Delaware, and Massachusetts 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), *cert. denied*, 139 S. Ct. 1373 (2019), the Ninth Circuit cited a routine, boilerplate warning that users should change their passwords, following a security breach, as evidence 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.

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*,[46] 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, consistent with pre-*Clapper* precedents from the Seventh and Ninth circuits. The Supreme Court's subsequent 6-2 compromise decision (by an 8-member Court) in *Spokeo, Inc. v. Robins*,[47] which occurred following the death of conservative Justice Antonin Scalia in early 2016, added yet another new standard for lower courts to apply in cases where standing is premised on breach of a federal statute. Both *Clapper* and

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

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

Spokeo were extended in 2021 by a more conservative Supreme Court—following the appointment of three new conservative justices by former President Trump—in *TransUnion LLC v. Ramirez*,[48] in which the Court, among other things, further tightened the standards for establishing Article III standing based on the threat of future harm, limited *Clapper* to cases involving injunctive relief, and held that the risk of future harm, without more, does not justify Article III standing.

27.07[2][B] Standing in Putative Cybersecurity Data Breach Consumer Class Action Suits in Chronological Context

Prior to *Clapper*, the Seventh[1] and Ninth[2] Circuits and district courts elsewhere[3] applied a more liberal standard

---

[48] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021).

[Section 27.07[2][B]]

[1] *See 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.

[2] *See 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

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[4] (along with various district courts (both before and after *Clapper*),[5] finding the threat of

---

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).

[3]*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).

[4]*See 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).

[5]*See, e.g., Browne v. US Fertility LLC,* Civil Action No. 21-367, 2021 WL 2550643, at *2-3 (E.D. Pa. June 22, 2021) (following *Reilly* in dismissing plaintiff's putative class action suit arising out of the theft of patient

personal information from Shady Grove Fertility clinics in Pennsylvania, Maryland, and New Jersey, holding that Browne's expenditure of $181.27 to purchase LifeLock services did not establish injury-in-fact and that he could "not achieve standing on the allegation that Defendants breached an implied contract or were unjustly enriched."); *Graham v. Universal Health Service, Inc.*, Civil Action No. 20-5375, 2021 WL 1962865, at *3-5 (E.D. Pa. May 17, 2021) (dismissing plaintiffs' putative class claims, arising out of a ransomware attack, for those plaintiffs whose injuries were premised on future risks and preventative measures, while denying defendant's motion to dismiss brought by the one plaintiff who alleged that his insurance premiums were increased as a result of the attack; "The target of a ransomware attack is the holder of the confidential data; the misappropriation of the data, whether by theft or merely limitation on access to it, is generally the means to an end: extorting payment. A court is still left to speculate, as in *Reilly*, whether the hackers acquired Plaintiffs' PHI in a form that would allow them to make unauthorized transactions in their names, as well as whether Plaintiffs are also intended targets of the hackers' future criminal acts."); *Springmeyer v. Marriott International, Inc*., Case No. 20-cv-867-PWG, 2021 WL 809894, at *3-4 (D. Md. Mar. 3, 2021) (dismissing plaintiffs' putative cybersecurity breach class action with prejudice where plaintiffs could not allege facts to show injuries fairly traceable to Marriott's alleged conduct; "mere repetition of conclusory and nonspecific allegations of Marriott's alleged shortcomings does not overcome the need to plead sufficient facts relating to what it did or did not do that led to the injuries claimed by the Plaintiffs. What is missing are any alleged facts to support these conclusory statements. For example, Plaintiffs do not allege any facts about what measures Marriott did or did not take to protect PII, what alleged inadequacies in its systems it should have disclosed, what 'standard and reasonably available steps' existed that Marriott did not take, how Marriott failed to detect the data breach, or why it did not provide timely and accurate notice of the breach."); *Clemens v. ExecuPharm, Inc.*, Civil Action No. 20-3383, 2021 WL 735728, at *3-5 (E.D. Pa. Feb. 25, 2021) (following *Reilly* in dismissing plaintiff's claims arising out of a ransomware attack undertaken by CLOP, for lack of standing, where plaintiff, a former employee, had her information (including her Social Security number, banking information (a copy of a personal check for direct deposit), driver's license, date of birth, home address, spouse's name, beneficiary information (including Social Security numbers) and payroll tax forms (such as W-2 and W-4)) stolen and released on the dark web, which she had argued evidenced that harm was certainly impending, despite alleging that she experienced actual harm from her time, money and effort to protect her information based on the imminent risks she allegedly faced, and that she alleged harm to her private contract rights); *Rahman v. Marriott International, Inc.*, Case No. SA CV 20-00654-DOC-KES, 2021 WL 346421 (C.D. Cal. Jan. 12, 2021) (dismissing plaintiff's complaint under the California Consumer Privacy Act and for breach of contract, breach of implied contract, unjust enrichment and unfair competition, for lack of Article III standing, in a suit arising out of Russian employees accessing putative class members' names, addresses, and other publicly available information, because the sensitivity of personal information, combined with its theft, are prerequisites to finding

that a plaintiff adequately alleged injury in fact); *In re Rutter's Inc. Data Security Breach Litigation*, 511 F. Supp. 3d 514 (M.D. Pa. 2021) (applying *Reilly* in holding that plaintiffs could not establish standing where their credit card information had been exposed but they had not incurred any loss; "As in *Reilly*, the harm that Plaintiffs . . . may face in the future—even if that harm is arguably more likely to occur than in *Reilly*—depends on multiple levels of impermissible speculation. To hold here that a plaintiff in a data breach class action, who has presently suffered no cognizable injury, can establish standing with allegations that she suffers some unquantifiable risk of future harm based on the lone fact that other people were harmed would totally undermine *Reilly*'s bright-line rule."); *Hartigan v. Macy's, Inc*., 501 F. Supp. 3d 1 (D. Mass. 2020) (dismissing putative class action claims premised on future harm, arising out of a data breach, for lack of Article III standing); *Stasi v. Inmediata Health Group Corp*., Case No.: 19cv2353 JM (LL), 2020 WL 2126317, at *4-10 (S.D. Cal. May 5, 2020) (dismissing plaintiffs' claims for negligence, negligence per se, breach of contract, violation of California's Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 to 56.37, and violation of the Minnesota Health Records Act, Minn. Stat. Ann. §§ 144.291 to 144.34, in a putative security breach class action suit arising out of a breach exposing medical records, for lack of Article III standing, where the type of information exposed, and resulting risk of identity theft, did not rise to a level sufficient to confer standing, where plaintiff did not allege that personal information was stolen or hacked, but merely made accessible via the Internet temporarily, and plaintiffs' information allegedly exposed did not include Social Security numbers or financial information); *Brett v. Brooks Bros. Group,* No. CV 17-4309-DMG (Ex), 2018 WL 8806668, at *4 (C.D. Cal. Sept. 6, 2018) (dismissing plaintiffs' claims for breach of implied contract, negligence, unlawful business practices under the California Unfair Competition Law, unfair business practices under the UCL, fraudulent/deceptive business practices under the UCL, and breach of covenant of good faith and fair dealing, in a putative data breach class action suit, for lack of Article III standing, where hackers allegedly stole plaintiffs' names, credit and debit card numbers (along with card expiration dates and verification codes) and possibly the Brooks Brothers store zip codes where plaintiffs made purchases as well as the time of those purchases, because "[t]his information simply does not rise to the level of sensitivity of the information in *Krottner* and *Zappos* or similar cases[;]" and dismissing plaintiffs' claim for an alleged violation of California's security breach notification law for lack of standing, premised on Brooks Brothers' disclosure about monitoring account statements, as required by California's security breach notification law, Cal. Civ. Code § 1798.82(d)(1), because "The Court will not interpret bare statutory compliance as an affirmative admission of imminent future harm. Indeed, such an interpretation would require courts to conclude that a data breach's mere occurrence establishes imminent risk of future harm, which is contrary to controlling Article III precedent, and it would perversely incentivize companies to provide vague or misleading disclaimers to customers affected by a data breach in an attempt to avoid litigation."); *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 secu-

rity 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 alleged that fake tax returns were submitted in plaintiff's name and a fraudulent account opened, because those injuries could not have been caused by the breach of social security, bank account, and routing numbers; "Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no . . . credible risk of identity theft that risks real, immediate injury."); *In re: Community Health Systems, Inc*., *Customer Security Data Breach Litigation*, No. 15-CV-222-KOB, 2016 WL 4732630, at *6-19 (N.D. Ala. Sept. 12, 2016) (granting in part defendant's motion to dismiss for lack of standing; "for the Plaintiffs in the instant case who did not have allegations of misuse accompanying their claims of an increased risk of harm, the facts pled here do not meet the definition of injury-in-fact; the alleged injuries are 'conjectural and hypothetical' and are not 'concrete,' nor are they 'actual or imminent.' "); *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1281–82 (M.D. Fla. 2016) (dismissing plaintiff's claim for lack of standing where plaintiff alleged two unauthorized charges (but, unlike in a subsequently amended pleading in the same case, did not allege actual out of pocket expense); "Plaintiff has not alleged that the two fraudulent charges went unreimbursed by his credit union and has experienced no additional actual harm since then."); *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); *Storm v. Paytime, Inc*., 90 F. Supp. 3d 359, 364-68 (M.D. Pa. 2015) (holding that employees lacked standing to sue over a cyber-attack that had occurred a year earlier but not resulted in any actual misuse of data, and that incurring costs to take certain precautions following the breach was not an injury in fact, and that the attack did not establish standing invasion of a privacy right; "the Third Circuit requires its district courts to dismiss data breach cases for lack of standing unless plaintiffs allege actual misuse of the hacked data or specifically allege how such misuse is certainly impending. Allegations of increased risk of identity theft are insufficient to allege a harm. . . . Plaintiffs argue that the different verbs used in their allegations, such as 'stolen' and 'misappropriated,' distinguish their case from *Reilly* in such a way as to create a cognizable harm, but this is a strained argument, which would require the Court to ignore the substance of the allegations."); *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 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,*

future harm to be too speculative to support standing, absent additional facts.

In *Reilly v. Ceridian Corp.*,[6] 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, 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."[7] 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 depen-

---

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.").

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

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

dent on the skill and intent of the hacker."[8]

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."[9] Similarly, standing in environmental injury cases is unique "because monetary compensation may not adequately return plaintiffs to their original position."[10] 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."[11]

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 basis for Appellants' claims."[12]

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,*[13] the First Circuit distinguished both the Third Circuit's holding in *Ceridian*[14] and Seventh and Ninth Circuit

---

[8]*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.*

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

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

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

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

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

[14]*Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied,* 566

opinions finding standing in data breach suits,[15] 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.[16]

Similarly, in *Frezza v. Google Inc.*,[17] a district court case, the court, in dismissing a breach of implied contract claim 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*,[18] emphasized that to establish standing

---

U.S. 989 (2012).

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

[16]*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).

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

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

"allegations of possible future injury are not sufficient."[19] The threatened injury must be "certainly impending" to constitute injury in fact.[20] 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,[21] 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.[22]

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.[23] As one court observed after *Clapper*, under current pleading standards it

---

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

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

[21]50 U.S.C.A. § 1881a.

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

[23]*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 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).

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."[24]

Courts in some jurisdictions that previously had more permissive standing rules, however, construed *Clapper* in security breach cases consistently with pre-*Clapper* circuit court law, rather than as a case that tightened the requirements for establishing Article III standing in a case based on the threat of future harm.

In *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[25] 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*.,[26] 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.' "[27]

Thereafter, in September 2014, in what at first appeared to be an aberrational opinion that eventually proved influential, Ninth Circuit Judge Lucy Koh (while she was still a district court judge in the Northern District of California) ruled in *In re Adobe Systems, Inc. Privacy Litigation*[28] that plaintiffs whose information had been compromised but who had not been victims of identity theft had standing to bring

---

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

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

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

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

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

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."[29] 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 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

[29] *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).

> 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.[30]

In the alternative, she ruled that even if *Krottner v. Starbucks Corp.*[31] was "no longer good law, the threatened harm alleged . . . [in *Adobe* was] sufficiently concrete and imminent to satisfy *Clapper*."[32] 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 to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so."[33] In so ruling,

---

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

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

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

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

Judge Koh distinguished *Polanco v. Omnicell, Inc.*,[34] 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.*[35] and *In re Barnes & Noble Pin Pad Litigation,*[36] 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.,*[37] 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."[38] 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? . . . ."[39] 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 and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly

---

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

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

[36]*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).

[37]*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*.

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

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

traceable' to the defendant's data breach."[40]

Judge Koh's analysis proved influential in *Remijas v. Neiman Marcus Group, LLC*,[41] 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."[42]

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 . . . ."[43]

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 was more imminent. In this regard, the fact that Neiman Marcus had offered a year of free credit monitoring services

---

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

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

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

[43]*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.

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*."[44] 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.[45]

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 monitoring in instances where it could help consumers deter identity theft, out of concern that doing so could increase a

---

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

[45] *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).

company's potential exposure in litigation. For this reason, other circuits have declined to draw this same inference[46] (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).[47]

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 diminished, which the panel characterized "some form of

---

[46] *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.

[47] *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.

unjust enrichment . . . ."[48]

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.[49] 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.*,[50] 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*.[51] 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 injuries that justified standing under *Remijas.* The future

---

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

[49]*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).

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

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

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) . . . ."[52]

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.[53] 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.[54] *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.[55]

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 courts in evaluating products that themselves were defective

---

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

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

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

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

or dangerous, which consumers claim they would not have bought.[56] Plaintiffs also alleged a property right to their personally identifiable information.[57]

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*.,[58] 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 Easterbrook, 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."[59] 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.[60]

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 sorting things out with the police and her bank, and (3) she

---

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

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

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

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

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

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.[61]

In an earlier case, *In re Target Corp. Data Security Breach Litigation*,[62] 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, and (4) continued to accept plaintiffs' credit and debit cards

---

[61] 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).

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

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,[63] to the extent available, while dismissing negligence claims under the laws of a number of states based on the economic loss rule.[64] 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.[65]

As an example of the more typical analysis undertaken following *Clapper,* but before *Spokeo*, in *In re SAIC Corp*.,[66] 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

---

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

[64]*See In re Target Corp. Data Security Breach Litigation*, 66 F. Supp. 3d 1154, 1171-76 (D. Minn. 2014).

[65]*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).

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

suffice to show causation, but the allegation that unsolicited telephone calls were received on a plaintiff's unlisted number from insurance companies and others targeted at her specific, undisclosed medical condition were sufficient.[67]

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."[68] 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.[69]

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-

---

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

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

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

tion could be in danger."[70] 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."[71]

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.' "[72] 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.").[73]

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."[74] 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

---

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

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

[72] *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).

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

[74] *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."[75] 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.[76]

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

---

[75] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410 (2013).

[76] *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*.[77]

In *Spokeo, Inc. v. Robins*,[78] 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 putative data security breach cases are brought under common law theories such as breach of contract, breach of implied contract, breach of fiduciary duty or negligence, federal statutes also may be asserted.[79]

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

---

[77]*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. 3d 359, 364–68 (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).

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

[79]By comparison, putative data privacy class action suits initially were brought primarily under federal statutes (although suits based on state law claims have become increasingly more significant). *See generally supra* § 26.15.

require a showing of actual harm.[80] Courts in the Ninth Circuit had construed this rule, first articulated in *Edwards v. First American Corp.*,[81] 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."[82]

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.[83]

---

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

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

[82]*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.

[83]*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

When the U.S. Supreme Court granted certiorari in the case then known as *Robins v. Spokeo, Inc.*,[84] 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 eight remaining members of the Court in 2016 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."[85] 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.[86] He further reiterated that the plaintiff bears this burden and, at the pleading stage, "must 'clearly . . . allege facts demonstrating' each element."[87] 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

---

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.").

[84] *See Robins v. Spokeo, Inc.*, 742 F.3d 409, 412-14 (9th Cir. 2014), *cert. granted*, 575 U.S. 982 (2015).

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

[86] *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).

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

conjectural or hypothetical.' "[88]

For an injury to be *particularized,* it "must affect the plaintiff in a personal and individual way."[89] 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.' "[90]

To be concrete, an injury must be " 'real' and not 'abstract.' "[91] It need not be *tangible,* however. "[I]ntangible injuries can . . . be concrete."[92]

In determining whether an intangible harm constitutes injury in fact, "both history and the judgment of Congress play important roles."[93] 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."[94] 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.' "[95]

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."[96] 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

---

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

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

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

[91]*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).

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

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

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

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

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

person a statutory right and purports to authorize that person to sue to vindicate that right."[97] For example, "a bare procedural violation, divorced from any concrete harm . . ." would not satisfy the injury-in-fact requirement.[98] 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 . . . ."[99]

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."[100]

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 left 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

---

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

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

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

[100] *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).

as actionable by English or American courts[101] or, for claims premised on federal statutes, one that Congress sought to elevate[102] to a concrete injury. For claims brought under

[101]*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 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."); *see also, e.g.*, *Fox v. Dakkota Integrated Systems, LLC*, 980 F.3d 1146, 1154-55 (7th Cir. 2020) (reversing the district court's order of remand, holding that plaintiff had standing to assert a BIPA section 15(a) claim against a former employer for failing to comply with data retention and destruction policies, holding that "[a]n unlawful retention of biometric data inflicts a privacy injury in the same sense that an unlawful collection does."); *Bryant v. Compass Group USA, Inc*., 958 F.3d 617 (7th Cir. 2020) (holding that Bryant had Article III standing to assert a claim under section 15(b) of BIPA, which requires a collector to inform those from whom it is collecting information that it is doing so, and to disclose the purpose of the collection and the length of the retention and obtain written consent from affected persons, because Bryant's allegations that Compass had violated section 15(b)'s requirement both to inform those from whom it was collecting data that it was doing so and why, and to obtain their written consent, was both concrete and particularized, while also finding that he lacked standing to bring a claim under section 15(a), in a suit over use of "Smart Market" vending machines owned by Compass, which required users to provide their fingerprints in connection with establishing an account); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 597-599 (9th Cir. 2020) (holding that plaintiffs had Article III standing to assert claims for invasion of privacy, intrusion upon seclusion, breach of contract, breach of implied contract, breach of the covenant of good faith and fair dealing, as well under the Wiretap Act and CIPA because they adequately alleged privacy harms, in a suit alleging that an app provider accessed user browsing history from third party apps, when they were logged out of the app, prior to 2011), *cert. denied*, 141 S. Ct. 1684 (2021); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274-75 (9th Cir. 2019) (affirming that plaintiffs established Article III standing based on an alleged Illinois BIPA violation), *cert. denied*, 140 S. Ct. 937 (2020).

[102]*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); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 597-601 (9th Cir. 2020) (holding that plaintiffs had Article III standing to assert claims for invasion of privacy, intrusion upon seclusion, breach of contract, breach of implied contract, breach of the covenant of good faith and fair dealing, as well under the Wiretap Act and CIPA because they adequately alleged privacy harms and because Congress intended to protect historic rights, and for common law trespass, fraud, statutory larceny, and violations of the CDAFA, in a suit alleging that an app provider accessed user browsing history from third party apps, when they were logged out of the app, prior to 2011), *cert. denied*, 141 S. Ct. 1684 (2021); *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*, 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

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),[103] the Cable

---

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).

[103]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 and no identity thief was there to snatch it, it did not make an injury."); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (en banc) (holding that plaintiff lacked Article III standing in a suit alleging that Godiva violated FACTA by printing too many digits on credit card receipts, thereby allegedly exposing customers to an elevated risk of identity theft; rejecting the argument that time spent destroying or

Communications Privacy Act,[104] other privacy statutes,[105]

---

safeguarding receipts in an effort to mitigate future harm amounted to anything more than a "hypothetical future harm" under *Clapper*); *see also Daniel v. National Park Service*, 891 F.3d 762, 766-68 (9th Cir. 2018) (distinguishing the Ninth Circuit's decision in *Bassett*, 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).

[104]*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.").

[105]*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

and other federal[106] and state[107] laws). Standing to assert

---

conducting anything other than a face scan where plaintiffs had to place 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); *Cordoba v. DirecTV, LLC*, 942 F.3d 1259 (11th Cir. 2019) (holding that plaintiffs whose phone numbers were not on the National Do Not Call Registry and never asked Telcel not to call them again lacked Article III standing for unwanted calls received from Telcel, under the TCPA, because the receipt of a call was not traceable to Telcel's alleged failure to comply with regulations requiring it to maintain an internal do-not-call list); *Salcedo v. Hanna*, 936 F.3d 1162, 1166-73 (11th Cir. 2019) (holding that a law firm client did not establish a concrete injury in fact from receiving a single unsolicited text message and, therefore, did not have Article III standing to sue under the Telephone Consumer Protection Act in federal court); *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.").

[106]*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).

[107]*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' "); *Miller v. Southwest Airlines Co.*, 926 F.3d 898, 902-03 (7th Cir. 2019) (holding that plaintiffs had Article III standing to sue under the Illinois Biometric Information Privacy Act (BIPA)); *Nicklaw v. 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); *Rahman v. Marriott International, Inc.*, Case No. SA CV 20-00654-DOC-KES, 2021 WL 346421 (C.D. Cal. Jan. 12, 2021) (dismissing plaintiff's complaint under the California Consumer Privacy Act (and for breach of contract, breach of implied contract, unjust enrichment and unfair competition), for lack of Article III standing, in a suit arising out of Russian employees accessing putative class members' names, addresses, and other publicly available information, because the sensitivity of personal information, combined with its theft, are prerequisites to finding that a plaintiff adequately alleged injury in fact); *Brett v. Brooks Bros. Group*, No. CV 17-4309-DMG (Ex), 2018 WL 8806668, at *4 (C.D. Cal. Sept. 6, 2018) (dismissing plaintiffs' claims for unfair competition under California law, in a putative data breach class action suit, for lack of Article III standing, where hackers allegedly stole plaintiffs' names, credit and debit card numbers (along with card expiration dates and verification codes) and possibly the Brooks Brothers store zip codes where plaintiffs made purchases as well as the time of those purchases, because "[t]his information simply does not rise to the level of sensitivity of the information in *Krottner* and *Zappos* or similar cases[;]" and dismissing plaintiffs' claim for an alleged violation of California's security breach notification law for lack of standing, premised on Brooks Brothers' disclosure about monitoring account statements, as required by California's security breach notification law, Cal. Civ. Code § 1798.82(d)(1), because "The Court will not interpret bare statutory compliance as an affirmative admission of imminent future harm. Indeed, such an interpretation would require courts to conclude that a data breach's mere occurrence establishes imminent risk of future harm, which is contrary to controlling Article III precedent, and it would perversely incentivize companies to provide vague or misleading disclaimers to customers affected by a data breach in an attempt to avoid litigation."); *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 alleged that fake tax returns were submitted in plaintiff's name and a fraudulent account opened, because those injuries could not have been caused by the breach of social security, bank account, and routing numbers); *Murray v. Lifetime Brands, Inc.,* Civil Action No.

state law claims presumably should be more limited—since Congress, which does not enact state laws, by definition could not elevate a state law claim to one justifying standing (although courts often treat state statutory claims as though they were federal claims in applying *Spokeo* and its progeny).

Spokeo's impact on putative data privacy and TCPA class action suits is addressed in sections 26.15 and 29.16, respectively.

Following *Spokeo,* the Sixth Circuit, in *Galaria v. Nationwide Mutual Insurance Co.*,[108] 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

---

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].

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

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 Nationwide recommended but did not cover.[109] 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

[109]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.

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.[110]

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.*[111] 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 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

---

[110]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).

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

cases, including the Sixth Circuit's own previous decision in *Lambert v. Hartman*,[112] 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*.,[113] as decisions that "completely ignore[d] the independent third party criminal action breaking the chain of causation."

In *Attias v. Carefirst, Inc*.,[114] 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 Carefirst 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 standing to sue based on their heightened risk of identity theft.[115]

The D.C. Circuit cited with approval the Seventh Circuit's decision in *Remijas v. Neiman Marcus Group, LLC*,[116] in concluding that it was plausible to infer that a party accessing plaintiffs' personal information did so with "both the

---

[112]*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).

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

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

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

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

intent and ability to use the data for ill."[117] 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.' "[118] 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."[119] 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."[120]

The D.C. Circuit also found standing in a subsequent data breach case.[121]

---

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

[118]*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).

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

[120]*Attias v. Carefirst, Inc.*, 865 F.3d 620, 626-27 (D.C. Cir. 2017) (quoting *Susan B. Anthony List v. Diehaus*, 573 U.S. 149, 157-58 (2014)), *cert. denied*, 138 S. Ct. 981 (2018).

[121]*See In re U.S. Office of Personnel Management Data Security Breach Litig.*, 928 F.3d 42, 54-61 (D.C. Cir. 2019). In that case, the D.C. Circuit reversed the lower court's order dismissing plaintiffs' suit arising out of an attack by unknown cyberattackers on databases 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 past, present, and prospective government employees. Plaintiffs alleged that the OPM had failed to comply with the Federal Information Security Management Act of 2014, which exposed plaintiffs to a higher risk of identity theft and other injuries.

The district court had focused on the lack of financial injury, opining that "[w]hile 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

Although *Attias* was decided in August 2017, the court did

. . . ." *U.S. Office of Personnel Management Data Security Breach Litig.*, 266 F. Supp. 3d 1, 19-26 (D.D.C. 2017), *rev'd*, 928 F.3d 42, 54-61 (D.C. Cir. 2019).

A majority of the D.C. Circuit panel, however, disagreed, and, applying earlier circuit case law, ruled that "the risk of future identity theft" constituted a concrete and particularized injury. 928 F.3d at 55, *citing Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017); *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (offering the "increased risk of fraud or identity theft" as an example of a "concrete consequence" in evaluating standing). The appellate panel contrasted *Beck v. McDonald*, 848 F.3d 262 (4th Cir.), *cert denied*, 137 S. Ct. 2307 (2017) and *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied*, 566 U.S. 989 (2012), where courts in other circuits found the risk of identity theft too speculative, because plaintiffs in *OPM* alleged that the cyberattackers intentionally targeted their information and pointed to subsequent misuse of that information. 928 F.3d at 58.

Judge Williams dissented, arguing that the fact that "sophisticated" cyberintruders spent several months systematically and covertly extracting 21.5 million highly sensitive background investigation records of federal government employees might have been undertaken by identity thieves, but with the passage of two years, he wrote that plaintiffs' "garden-variety identity theft theory lack[ed] plausibility in light of an obvious alternative explanation: . . . the handiwork of foreign spies looking to harvest information about millions of federal workers for espionage or kindred purposes having nothing to do with identity theft." 928 F.3d at 75-76 (Williams, J. dissenting). Judge Williams disagreed with the majority that standing could be justified based on alternatively plausible theories of the basis for the cyberattack, concluding that plaintiffs had not alleged sufficient facts to negate this alternative explanation. He also discounted the fact that some plaintiffs had had fraudulent accounts opened and tax returns filed in their names, noting that in a society where approximately 3.3% of the population will experience some form of identity theft in a given year, it was not surprising that a few plaintiffs in a putative class of 21.5 million would have experienced some form of fraud. *Id.* at 79 (Williams, J. dissenting). By comparison, he speculated that a handful of plaintiffs "almost certainly experienced a home invasion since the data breach. But that doesn't imply a 'substantial risk' that *these hackers* have plans to break into the homes of garden-variety government employees." *Id.* (emphasis in original). Except for those who actually experienced financial fraud, Judge Williams argued that Article III standing was lacking.

The majority accepted the general principle that threatened injuries become more speculative as breaches fade further into the past, but viewed the passage of two years as less significant in *OPM* because it was not a "run-of-the-mill data breach case . . . . Conducted over several months by sophisticated and apparently quite patient cyberhackers, the attacks at issue in this case affected over twenty-one million people and involved information far more sensitive than credit card numbers." 928 F.3d at 59. The majority conceded that the breach did not expose "all information necessary to make fraudulent charges on the victims' existing financial ac-

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.*[122] and *Beck v. McDonald*.[123]

In *Whalen v. Michaels Stores, Inc.*,[124] 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 Secu-

---

counts, [but] the personal data the hackers did manage to obtain is enough, by itself, to enable several forms of identity theft. That fact, combined with the allegations that at least some of the stolen information was actually misused after the breaches, suffices to support a reasonable inference that . . . plaintiffs' risk of identity theft is traceable to the OPM cyberattacks." *Id.* at 60.

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

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

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

rity 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."[125]

In *Beck v. McDonald*,[126] the Fourth Circuit held that patients at a Veterans Affairs hospital who sued under the Privacy Act[127] and Administrative Procedure Act[128] 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.[129] The court also rejected the argument that the cost of mitigation measures provided grounds for standing.[130]

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."[131]

In the companion *Watson* case, identifying information of

---

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

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

[127]5 U.S.C. §§ 552a *et seq*.

[128]5 U.S.C. §§ 701 *et seq*.

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

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

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

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 injury was "certainly impending."[132] 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 findings of no injury-in-fact in eboth cases, 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.' "[133] 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."[134] 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 infor-

---

[132]*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.

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

[134]*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).

mation, "without more, cannot confer Article III standing."[135] The appellate panel distinguished cases applying the more liberal Seventh Circuit test because those cases involved a data thief intentionally targeting personal information that was compromised in a breach.[136] The court also differentiated cases where at least one named plaintiff alleged misuse or access by the thief.[137] 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."[138] The court explained that " 'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative."[139] To assume that plaintiffs would in fact suffer identity theft, the court

---

[135]*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 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).

[136]*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).

[137]*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).

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

[139]*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*

explained, would require engaging "in the same 'attenuated chain of possibilities' rejected by the [Supreme] Court in *Clapper*."[140] 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.[141]

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 posi-

---

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), *cert. denied*, 139 S. Ct. 1373 (2019).

[140]*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.

[141]*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.

tion completely.' "[142]

The Fourth Circuit panel acknowledged that standing may be found where there is a "substantial risk" that harm would occur, which in turn may cause a party to reasonably incur costs to mitigate or avoid that harm, but ruled that was not the case in *Beck*.[143]

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."[144] 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."[145]

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).[146] The Fourth Circuit explained that:

Contrary to some of our sister circuits, we decline to infer a

---

[142]*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).

[143]*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).

[144]*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).

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

[146]*See Galaria v. Nationwide Mutual Insurance Co.,* 663 F. App'x 384, 388 (6th Cir. 2016) ("Indeed, Nationwide seems to recognize the severity of

> 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.[147]

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."[148]

The year after *Beck,* a Fourth Circuit panel that included two of the three judges that decided *Beck* found Article III standing to be proper in *Hutton v. National Board of Examiners in Optometry, Inc*.[149] In *Hutton*, the panel reaffirmed the principles from *Beck* that "a plaintiff fails to 'es-

---

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.").

[147]*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.

[148]*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).

[149]*Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018). *Beck* was written by Judge Albert Diaz, joined by Judge Paul V. Niemeyer and West Virginia District Court Judge Irene M. Keeley, sitting by designation. *Hutton* was written by Judge Robert Bruce

tablish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it.' . . . [And] a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft."[150] The *Hutton* panel, however, considered the case before it to be readily distinguishable from *Beck,* where plaintiffs had alleged a threat of future injury where a laptop and boxes containing patient records (including partial Social Security numbers, names, dates of birth, and physical descriptions) had been stolen but the information had not been misused. By contrast, in *Hutton,* the plaintiffs, along with other optometrists across the United States, noticed that Chase Amazon Visa card accounts had been fraudulently opened in their names and plaintiffs (two of whom had discovered cards opened in their maiden names) traced the scams back to the National Board of Examiners in Optometry, which they believed was the only common source to which they and other optometrists had provided their personal information (including Social Security numbers, names, dates of birth, addresses, and credit card information). Although they had not alleged that they had incurred fraudulent charges themselves (merely the costs for mitigation measures to safeguard against future identity theft), plaintiffs had, in the Fourth Circuit panel's words, "sufficiently alleged an imminent threat of injury to satisfy Article III standing" by alleging that "that they have already suffered actual harm in the form of identity theft and credit card fraud. The Plaintiffs have been concretely injured by the data breach because the fraudsters used—and attempted to use—the Plaintiffs' personal information to open Chase Amazon Visa credit card accounts without their knowledge or approval. . . . Here, the Plaintiffs allege that their data has been stolen, accessed, and used in a fraudulent manner."[151] In *Beck,* the *Hutton* panel explained, the threat was speculative because even after extensive discovery there was no evidence that the information contained on a stolen laptop had been accessed or misused or that the plaintiffs

---

King, joined by Judges Diaz and Niemeyer from the *Beck* panel.

[150] *Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018), *quoting Beck v. McDonald*, 848 F.3d 262, 266 (4th Cir.), *cert denied*, 137 S. Ct. 2307 (2017).

[151] *Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018).

had suffered identity theft.[152]

The *Hutton* panel found plaintiffs' mitigation expenses—out-of-pocket costs, lost time, and credit monitoring services—sufficient to establish injury-in-fact because the injuries alleged were not speculative. It explained that "although incurring costs for mitigating measures to safeguard against future identity theft may not constitute an injury-in-fact when that injury is speculative, *see Beck*, 848 F.3d at 276, the Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists . . . ."[153]

The Fourth Circuit panel in *Hutton* also addressed traceability, concluding that it was "both plausible and likely that a breach of the NBEO's database resulted in the fraudulent use of the Plaintiffs' personal information, resulting in their receipt of unsolicited Chase Amazon Visa credit cards."[154]

---

[152]*Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018).

[153]*Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018), *citing Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409, 414 n.5 (2013).

[154]*Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613, 623 (4th Cir. 2018). The panel explained:

> The Complaints allege that a group of optometrists from around the country began to notice that fraudulent Chase accounts were being opened in their names in July 2016. For example, in August 2016, Hutton and Kaeochinda received their unsolicited Chase Amazon Visa credit cards. Hutton's fraudulent credit card was applied for in her maiden name—which she had provided to the NBEO eighteen years earlier. Kaeochinda's unsolicited Chase credit card was applied for in her former married name, which she had provided to the NBEO several years earlier. In August 2016, Mizrahi was informed by a credit monitoring service of an effort to open a fraudulent credit card account in her name, using personal information she had previously provided to the NBEO in registering for a professional examination. Notably, the Plaintiffs allege that, amongst the group of optometrists, the NBEO is the only common source that collected and continued to store social security numbers that were required to open a credit card account, and also stored outdated personal information (such as maiden names and former married names) during the relevant time periods. Furthermore, other national optometry organizations do not gather or store Social Security numbers, or have investigated and confirmed that their databases have not been breached.

Id. As the panel concluded: "Put simply, the Complaints contained sufficient allegations that the NBEO was a plausible source of the Plaintiffs' personal information." *Id.*

The case ultimately settled on remand. *See Hutton v. National Board of Examiners in Optometry, Inc.*, Civil Nos. JKB-16-3025, JKB-16-3146, JKB-17-19642019, WL 3183651 (D. Md. July 15, 2019) (granting final approval of a class action settlement).

In 2017, in *In re SuperValu, Inc., Customer Data Security Breach Litigation*,[155] 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.[156] In *SuperValu,* the defendants experienced two separate security breaches, which they announced in press 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.[157] 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

---

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

[156]*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 773 (citing *Lexmark Int'l, Inc. v. Static Control Components, Inc.,* 572 U.S. 118, 134 n.6 (2014) ("Proximate causation is not a requirement of Article III standing.")).

On remand, the claims of the one plaintiff who had alleged incurred a fraudulent charge were dismissed for failure to state a claim. *See In re SuperValu, Inc., Customer Data Security Breach Litig.*, 925 F.3d 955 (8th Cir. 2019) (affirming dismissal of claims).

[157]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).

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.[158]

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 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.[159]

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.[160] While stolen card data could be used to commit credit or debit card fraud, the GAO report

---

[158]*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,* 573 U.S. 149, 157-58 (2014); *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409, 414 n.5 (2013)).

[159]*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)).

[160]*In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870

did not "plausibly support the contention that consumers affected by a data breach face a substantial risk of credit or debit card fraud."[161] The GAO report concluded that "based on the 'available data and information . . . most breaches have not resulted in detected incidents of identity theft.' "[162] Accordingly, the court found there was no standing, explaining that "a mere possibility is not enough for standing."[163]

The Eighth Circuit panel also rejected the argument that the costs incurred to mitigate the risk of identity theft, 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."[164]

In 2018, the Ninth Circuit, in *In re Zappos.com, Inc*.,[165] reaffirmed its pre-*Clapper* liberal rule of standing from *Krottner v. Starbucks Corp*.,[166] 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

---

F.3d 763, 770 (8th Cir. 2017).

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

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

[163]*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.").

[164]*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)).

[165]*In re Zappos.com, Inc.,* 888 F.3d 1020, 1023-30 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).

[166]*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).

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*, *TransUnion* and *Spokeo.* The fact that *other people* incurred a financial loss in reality doesn't make it more likely that the plaintiffs in *Zappos* would as well.[167]

In ruling as it did, the panel distinguished the Fourth Circuit's admonition in *Beck v. McDonald*[168] 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.[169]

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 *Super-*

---

[167] *But see In re U.S. Office of Personnel Management Data Security Breach Litig.*, 928 F.3d 42, 54-61 (D.C. Cir. 2019) (concluding that fraudulent account activity encountered by some plaintiffs justified the inference that all 21.5 million putative plaintiffs suffered a risk of future identity theft).

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

[169] *In re Zappos.com, Inc.,* 888 F.3d 1020, 1028-29 & n.13 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).

Valu 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).[170]

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

Thereafter, in 2021, the Eleventh Circuit, in *Tsao v. Captiva MVP Restaurant Partners, LLC*,[171] following the Eighth Circuit in *SuperValu,* affirmed dismissal of plaintiff's breach of implied contract, negligence, unjust enrichment, unfair competition, and other related claims, arising out of the data breach of a restaurant's point of sale system, which allegedly exposed plaintiff's (and other customers') credit card and other financial information. In that case, Tsao alleged three types of injuries suffered in his efforts to mitigate the perceived risk of future identity theft: lost cash back or reward points (due to lost use from canceling and waiting for reissued credit cards), lost time spent addressing the problems caused by the cyber-attack, and restricted card access resulting from his credit card cancellations).

Former Chief Judge Gerald Bard Tjoflat, writing for the majority (with one judge concurring[172]), characterized Tsao's arguments as focusing on two general theories of standing, both of which the court rejected: "First, he argues that he *could* suffer future injury from misuse of the personal information disclosed during the cyber-attack (though he has not yet), and this risk of misuse alone is enough to satisfy the standing requirement. Then, he argues that he has *already*

---

[170] *In re Zappos.com, Inc.,* 888 F.3d 1020, 1026 n.6 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).

[171] *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021).

[172] Judge Jordan concurred in the result given circuit precedent—*Muransky v. Godiva Chocolatier, Inc*., 979 F. 3d 917 (11th Cir. 2020) (en banc), from which he had dissented—but cautioned that the majority, "rather than viewing Mr. Tsao's allegations favorably, necessarily engage[d] in a value-laden and normative inquiry concerning the question of "substantial risk" at the motion-to-dismiss stage." *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1345 (11th Cir. 2021) (Jordan, J. concurring). He wrote that, "[h]opefully the Supreme Court will soon grant certiorari in a case presenting the question of Article III standing in a data breach case." *Id.*

suffered some 'concrete, particularized' mitigation injuries—for example, lost time, lost rewards points, and loss of access to accounts—that are sufficient to confer standing."[173] Distilling *Clapper* and prior circuit court case law interpreting it, Judge Tjoflat wrote that

> we can distill two legal principles relevant to Tsao's claims. First, a plaintiff alleging a threat of harm does not have Article III standing unless the hypothetical harm alleged is either "certainly impending" or there is a "substantial risk" of such harm. . . . Second, if the hypothetical harm alleged is not "certainly impending," or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk.[174]

Surveying circuit court case law, Judge Tjoflat rejected plaintiff's " 'elevated risk of identity theft' theory . . . ," observing that "[g]enerally speaking, the cases conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse or actual access to personal data."[175] Agreeing with the Eighth Circuit in *SuperValu,* where the court found that the sole plaintiff who alleged actual misuse had standing based on present, not future injury, and that the other plaintiffs could not establish standing where the hackers were not alleged to have stolen social security numbers, birth dates, or driver's license numbers, and thus, the risk of identity theft was deemed to be negligible, Judge Tjoflat reasoned:

> Here, as the plaintiffs did in *SuperValu*, Tsao has alleged that hackers *may* have accessed and stolen customer credit card data "including the cardholder name, the account number, expiration date, card verification value ('CVV'), and PIN data for debit cards." And here, just like the plaintiffs in *SuperValu*, Tsao cites to the 2007 GAO Report on data breaches in support of his theory that the PDQ hack may result in future identity theft. But we, like the Eighth Circuit in *SuperValu*, believe the GAO Report actually demonstrates why there is no "substantial risk" of identity theft here. Tsao has not alleged that social security numbers, birth dates, or driver's license numbers were compromised in the PDQ breach, and the card information allegedly accessed by the PDQ hackers "generally

---

[173] *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1337 (11th Cir. 2021) (emphasis in original).

[174] *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1339 (11th Cir. 2021) (citations and footnote omitted).

[175] *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1340-41 (11th Cir. 2021).

> cannot be used alone to open unauthorized new accounts." GAO Report at 30. So, based on the GAO Report, it is unlikely that the information allegedly stolen in the PDQ breach, standing alone, raises a substantial risk of identity theft.
>
> This leaves us with the risk that the hackers, if they accessed and stole Tsao's credit card information, could make unauthorized purchases with his cards or drain his accounts. But again, the GAO Report suggests that most data breaches have not resulted in detected incidents of fraud on existing accounts. *See id.* at 21. Indeed, the GAO Report reviewed the 24 largest data breaches between January 2000 and June 2005 and found that only 4 of the 24 breaches (roughly 16.667%) resulted in some form of identity theft, and only 3 resulted in account theft or fraud (12.5%). *Id.* at 24–25. Given the low rate of account theft, the GAO Report simply does not support the conclusion that the breach here presented a "substantial risk" that Tsao would suffer unauthorized charges on his cards or account draining.[176]

With respect to Tsao's alleged present injuries, the majority rejected the time and inconvenience incurred in canceling credit cards, writing that "[i]t is well established that plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.' "[177]

Also in 2021, the Second Circuit, in *McMorris v. Carlos Lopez & Associates, LLC*,[178] affirmed the dismissal of plaintiff's suit for lack of standing where the defendant accidently sent an email to all of its approximately 65 employees attaching a spreadsheet containing the sensitive PII (including Social Security numbers, home addresses, birth dates, phone numbers, educational degrees, and dates of hire) of approximately 130 then-current and former employees, where plaintiffs failed to allege that their PII was subject to a targeted data breach or allege any facts suggest-

---

[176] *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1342-42 (11th Cir. 2021). The court also emphasized the conclusory nature of plaintiff's allegations of an elevated risk and the fact that "Tsao immediately cancelled his credit cards following disclosure of the PDQ breach, effectively eliminating the risk of credit card fraud in the future. Of course, even if Tsao's cards are cancelled, some risk of future harm involving identity theft (for example, the use of Tsao's name) still exists, but that risk is not substantial and is, at best, speculative." *Id.* at 1344.

[177] *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021), *quoting Clapper v. Amnesty International USA*, 568 U.S. 398, 416 (2013).

[178] *McMorris v. Carlos Lopez & Associates, LLC,* 995 F.3d 295, 299-305 (2d Cir. 2021).

ing that their PII (or that of any other similarly situated people) was misused, and hence failed to allege that they were at a substantial risk of future identity theft or fraud sufficient to establish Article III standing. Nevertheless, the Second Circuit panel wrote in *McMorris* that a plaintiff *may* establish Article III standing based on an "increased risk" of future harm in appropriate circumstances, and sought to articulate a standard for when increased risk would justify Article III standing in future cases by attempting to harmonize divergent case law from the different circuits.

Attempting to synthesize data breach standing case law notwithstanding a substantial circuit split, the *McMorris* court ruled that

> courts confronted with allegations that plaintiffs are at an increased risk of identity theft or fraud based on an unauthorized data disclosure should consider the following non-exhaustive factors in determining whether those plaintiffs have adequately alleged an Article III injury in fact: (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.[179]

The panel reasoned that where plaintiffs have failed to present evidence or make any allegations that an unauthorized third party purposefully obtained the plaintiffs' data, courts have regularly held that the risk of future identity theft is too speculative to support Article III standing. "By contrast, where plaintiffs demonstrate that a malicious third party intentionally targeted a defendant's system and stole plaintiffs' data stored on that system, courts have been more willing to find that those plaintiffs have established a likelihood of future identity theft or fraud sufficient to confer standing."[180]

Explaining the second factor, the *McMorris* panel wrote that "while not a necessary component of establishing standing, courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where

---

[179] *McMorris v. Carlos Lopez & Associates, LLC,* 995 F.3d 295, 303 (2d Cir. 2021).

[180] *McMorris v. Carlos Lopez & Associates, LLC,* 995 F.3d 295, 301 (2d Cir. 2021).

they can show that at least some part of the compromised dataset has been misused—even if plaintiffs' particular data subject to the same disclosure incident has not yet been affected."[181]

Finally, with respect to the type of data involved, the panel cited to the Second Circuit's prior decision in *Whalen* in explaining that "courts have looked to the type of data at issue, and whether that type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed. Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth—especially when accompanied by victims' names—makes it more likely that those victims will be subject to future identity theft or fraud. . . . By contrast, less sensitive data, such as basic publicly available information, or data that can be rendered useless to cybercriminals does not pose the same risk of future identity theft or fraud to plaintiffs if exposed."[182]

The *McMorris* panel cautioned that standing is an "inherently fact-specific inquiry" and that these factors are "by no means the only ones relevant to determining whether plaintiffs have shown an injury in fact based on an increased risk of identity theft or fraud."[183]

The panel also addressed the question of whether stand-

---

[181]*McMorris v. Carlos Lopez & Associates, LLC,* 995 F.3d 295, 301 (2d Cir. 2021). In support of this point, the panel cited *In re Zappos.com, Inc.,* 888 F.3d 1020, 1027 & n.7 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019) and *In re U.S. Office of Personnel Management Data Security Breach Litig*., 928 F.3d 42, 58 (D.C. Cir. 2019) ("[A] hacker's 'intent' to use breach victims' personal data for identity theft becomes markedly less important where, as here, several victims allege that they have already suffered identity theft and fraud as a result of the breaches.") and *Fero v. Excellus Health Plan, Inc*., 304 F. Supp. 3d 333, 341, 344–45 (W.D.N.Y. 2018) (holding that allegations that the plaintiffs' PII was available for sale on the Dark Web following a data breach—and could therefore be purchased by cybercriminals at any moment to commit identity theft or fraud—provided strong support for the conclusion that those plaintiffs had established an Article III injury in fact). It is questionable whether this analysis remains valid in light of the U.S. Supreme Court's more recent opinion in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), rejecting standing for those who had not in fact been disclosed, in a case where other people's information had been disclosed to third parties (and those plaintiffs were deemed to have had standing).

[182]*McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 302 (2d Cir. 2021).

[183]*McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 302 (2d

ing may be based on plaintiffs having taken steps to protect themselves following an unauthorized disclosure, concluding unequivocally that those costs alone could not support a finding of injury in fact.[184] Relying on *Clapper,* the panel wrote that "where plaintiffs have shown a substantial risk of future identity theft or fraud, 'any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact.' . . . But where 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.' "[185]

Thus, the *McMorris* court articulated an amalgam of holdings from other circuits—trying to create cohesion where there is not necessarily any (except perhaps in the Second Circuit).

Applying this approach, the *McMorris* court found the case before it to present "a relatively straightforward situation in which Plaintiffs have failed to show that they are at a substantial risk of future identity theft or fraud sufficient to establish Article III standing."[186]

First, plaintiffs never alleged that their data was intentionally targeted or obtained by a third party outside of the defendant's company.

Second, plaintiffs did not allege that their data (or the data of any other then-current or former employees) "was in any way misused because of the accidental email. Again, while plaintiffs need not show that they have already experienced identity theft or fraud to adequately plead an Article III injury in fact, Plaintiffs do not allege any facts suggesting that their PII was misused following the accidental email here, which distinguishes this case from those in which plaintiffs have shown that some part of the exposed dataset was compromised."[187]

Third (and finally), the panel concluded that in the absence

Cir. 2021).

[184]*McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 303 (2d Cir. 2021).

[185]*McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 303 (2d Cir. 2021).

[186]*McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 303 (2d Cir. 2021).

[187]*McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 304 (2d Cir. 2021).

of any other facts suggesting that the PII was intentionally taken by an unauthorized third party or otherwise misused, the fact that the information that was "inadvertently disclosed included the sort of PII that might put Plaintiffs at a substantial risk of identity theft or fraud" could not alone establish an injury in fact; "To hold otherwise would allow plaintiffs to string together a lengthy 'chain of possibilities' resulting in injury."[188] In short, the panel concluded that "the sensitive nature of McMorris's internally disclosed PII, by itself, does not demonstrate that she is at a substantial risk of future identity theft or fraud. Because McMorris did not allege that her PII was subject to a targeted data breach or allege any facts suggesting that her PII (or that of any other similarly situated people) was misused, the district court correctly dismissed her complaint for failure to establish an Article III injury in fact."[189]

The *McMorris* panel further observed in *dicta* that although plaintiff did not press the alternative theory of injury in fact based on the time and money spent monitoring or changing their financial information and accounts, such a theory would have failed "for the simple reason that McMorris has failed to show that she is at a substantial risk of future identity theft, so 'the time [she] spent protecting [herself] against this speculative threat cannot create an injury.' "[190]

The *McMorris* court's ruling—in finding no Article III standing even in the face of the exposure of sensitive information—ultimately hues closely to *Clapper,* even as the court's articulation of the proper analysis for courts to employ, like the Fourth Circuit's, suggests some flexibility based on rulings from jurisdictions that take a more liberal approach to standing in cybersecurity data breach cases where the injury alleged is premised on future harm. The Seventh, Ninth, and D.C. Circuits (and the Sixth Circuit in an unreported opinion) take a more liberal view than *Clapper* would suggest, while the Second, Third (in an older case),

---

[188] *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 304 (2d Cir. 2021), *quoting Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 410 (2013).

[189] *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 304 (2d Cir. 2021).

[190] *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 304 n.7 (2d Cir. 2021), *quoting 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, 416 (2013)).

Fourth and Eighth Circuits adhere more closely to *Clapper* (although one could argue that the Second Circuit in *McMorris* and the Fourth Circuit in *Hutton* take a slightly more liberal approach in acknowledging the potential for standing to be found where an breach appears to have been targeted and where others may have experienced loss).

While *Tsao*, *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.

The infirmity of the Seventh, Ninth, and DC Circuit precedents (and Sixth Circuit's non-precedential opinion) on standing in putative cybersecurity breach class action suits where harm is premised on the risk of future injury was brought into sharp focus in June 2021 when the U.S. Supreme Court issued its 5-4 opinion in *TransUnion LLC v. Ramirez*.[191] *Ramirez* involved a trial verdict for a certified plaintiffs' class in a Fair Credit Reporting Act case, where the Supreme Court found that most of the class members lacked standing.

In *Ramirez*, the trial court had certified a class of 8,185 individuals who had OFAC alerts in their credit files. TransUnion offered customers an optional OFAC Name Screen Alert service, which identified individuals whose names were included on a list maintained by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) of suspected terrorists, drug traffickers and other serious criminals. Plaintiffs had alleged that TransUnion violated the Fair Credit Reporting Act by failing to use reasonable procedures to ensure the accuracy of their credit files. The Supreme Court, however, held that only 1,853 class members, including Ramirez, who had had OFAC alerts in their files communicated to third parties, had standing, because they had suffered a harm with a "close relationship" to the harm associated with the tort of defamation. By contrast, the remaining 6,332 class members whose files also contained misleading OFAC alerts did not have standing because their information was never communicated to a third party and "the mere existence of inaccurate information in a database

[191] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021).

is insufficient [absent dissemination] to confer Article III standing."[192] The Court also held that formatting errors in notices sent to all class members about the incorrect OFAC alerts did not justify standing because plaintiffs did not demonstrate that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts under *Spokeo*.[193]

Justice Kavanaugh, in a lengthy opinion that sought to do more than merely answer the narrow question presented about whether all class members in a certified class action were required to have standing,[194] framed the concrete-harm requirement to establish Article III standing as an issue that is essential to maintaining the separation of powers.[195] *Ramirez* tightened *Clapper* by limiting its application in

---

[192]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2209 (2021).

[193]*See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2213 (2021). Plaintiffs had argued that TransUnion breached its obligation to provide them their complete credit files upon request because it had sent copies that omitted the OFAC information and then sent a second mailing about OFAC which they argued should have included another summary of rights notice. The Supreme Court, however, held that these were bare procedural violations under *Spokeo,* writing that plaintiffs had

> not demonstrated that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts. *See Spokeo*, 578 U. S., at 341. In fact, they do not demonstrate that they suffered any harm at all from the formatting violations. The plaintiffs presented no evidence that, other than Ramirez, "a single other class member so much as *opened* the dual mailings," "nor that they were confused, distressed, or relied on the information in any way." . . . The plaintiffs put forth no evidence, moreover, that the plaintiffs would have tried to correct their credit files—and thereby prevented dissemination of a misleading report—had they been sent the information in the proper format.

TransUnion LLC v. Ramirez, 141 S. Ct. at 2213. The Court likewise rejected the argument that TransUnion's formatting violations created a risk of future harm. *See id.* at 2213-14. The Court also rejected the argument of the United States, as *amicus curiae*, that the plaintiffs suffered a concrete "informational injury" because "plaintiffs did not allege that they failed to receive any required information. They argued only that they received it *in the wrong format*." *Id.* at 2214 (emphasis in original).

[194]The specific question on which *cert.* had been granted was: "Whether either Article III or Rule 23 permits a damages class action where the vast majority of the class suffered no actual injury, let alone an injury anything like what the class representative suffered."

[195]*See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2206-07 (2021) ("the concrete-harm requirement is essential to the Constitution's separation of powers."). Among other things, Justice Kavanaugh wrote that a "regime where Congress could freely authorize *unharmed* plaintiffs to sue

most cases to suits for injunctive relief, not damages, holding that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial. . . . But . . . a plaintiff 's standing to seek injunctive relief does not necessarily mean that the plaintiff has standing to seek retrospective damages. . . . [I]n a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm."[196] And it tightened *Spokeo* by making clear that "*Spokeo* is not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts."[197]

Quoting an article by former Justice Antonin Scalia, Justice Kavanaugh wrote that a plaintiff, to have standing, must have a personal stake in the litigation, demonstrated by "sufficiently answer[ing] the question: 'What's it to you?' "[198]

"To answer that question in a way sufficient to establish standing, . . ." Judge Kavanaugh wrote, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief."[199] Justice Kavanaugh explained:

> Requiring a plaintiff to demonstrate a concrete and particularized injury caused by the defendant and redressable by the court ensures that federal courts decide only "the rights of individuals," *Marbury v. Madison*, 1 Cranch 137, 170 (1803), and that federal courts exercise "their proper function in a limited and separated government," Roberts, *Article III Limits on Statutory Standing*, 42 Duke L.J. 1219, 1224 (1993). Under

---

defendants who violate federal law not only would violate Article III but also would infringe on the Executive Branch's Article II authority." *Id.* at 2207 (emphasis in original).

[196] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210-11 (2021) (emphasis in original; citations omitted).

[197] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2204 (2021).

[198] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2203 (2021), *quoting* Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 Suffolk U.L. Rev. 881, 882 (1983).

[199] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2203 (2021).

> Article III, federal courts do not adjudicate hypothetical or abstract disputes. Federal courts do not possess a roving commission to publicly opine on every legal question. Federal courts do not exercise general legal oversight of the Legislative and Executive Branches, or of private entities. And federal courts do not issue advisory opinions. As Madison explained in Philadelphia, federal courts instead decide only matters "of a Judiciary Nature." 2 Records of the Federal Convention of 1787, p. 430 (M. Farrand ed. 1966).
>
> In sum, under Article III, a federal court may resolve only "a real controversy with real impact on real persons." *American Legion v. American Humanist Assn.*, 139 S. Ct. 2067, 2103 (2019).[200]

Justice Kavanaugh reiterated the principle from *Spokeo* that a concrete harm may be based on tangible harm and, in some circumstances, intangible. "[T]raditional tangible harms, such as physical harms and monetary harms . . . ," Justice Kavanaugh explained, readily qualify as concrete injuries under Article III.[201] "Chief among the[] ["[v]arious intangible harms [that] can also be concrete"] are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts . . . [such as], for example, reputational harms, disclosure of private information, and intrusion upon seclusion.[202]. . . . And those traditional harms may also include harms specified by the Constitution itself."[203] He also reiterated that, as *Spokeo* made clear, Congress's views may be "instructive."[204] Quoting a Sixth Circuit opinion, however, Justice Kavanaugh cautioned that

---

[200] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2203 (2021).

[201] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2204 (2021).

[202] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2204 (2021), *citing Spokeo, Inc. v. Robins,* 578 U.S. 330, 340–41 (2016), *Meese v. Keene*, 481 U.S. 465, 473 (1987) (reputational harms), *Davis v. Federal Election Commission*, 554 U.S. 724, 733 (2008) (disclosure of private information), and *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.) (intrusion upon seclusion); *see generally infra* §§ 26.15 (analyzing standing in data privacy cases), 29.16[6] (analyzing standing in texting and other TCPA cases and discussing *Gadelhak v. AT&T*).

[203] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2204, *citing Spokeo, Inc. v. Robins,* 578 U.S. 330, 340 (2016) (citing *Pleasant Grove City v. Summum*, 555 U.S. 460 (2009) (abridgment of free speech), and *Church of Lukumi Babalu Aye, Inc. v. Hialeah*, 508 U.S. 520 (1993) (infringement of free exercise)).

[204] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2204 (2021), *quoting Spokeo, Inc. v. Robins,* 578 U.S. 330, 341 (2016).

> even though "Congress may 'elevate' harms that 'exist' in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is." . . . Congress's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III any more than, for example, Congress's enactment of a law regulating speech relieves courts of their responsibility to independently decide whether the law violates the First Amendment. . . .
>
> For standing purposes, therefore, an important difference exists between (i) a plaintiff 's statutory cause of action to sue a defendant over the defendant's violation of federal law, and (ii) a plaintiff 's suffering concrete harm because of the defendant's violation of federal law. Congress may enact legal prohibitions and obligations. And Congress may create causes of action for plaintiffs to sue defendants who violate those legal prohibitions or obligations. But under Article III, an injury in law is not an injury in fact. Only those plaintiffs who have been concretely harmed by a defendant's statutory violation may sue that private defendant over that violation in federal court. As then-Judge Barrett succinctly summarized, "Article III grants federal courts the power to redress harms that defendants cause plaintiffs, not a freewheeling power to hold defendants accountable for legal infractions." *Casillas*, 926 F.3d at 332.[205]

The Supreme Court held unequivocally in *Ramirez* that

---

[205] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2205 (2021), *quoting Hagy v. Demers & Adams*, 882 F.3d 616, 622 (6th Cir. 2018) (Sutton, J.) (citing *Spokeo, Inc. v. Robins,* 578 U.S. 330, 341 (2016)). Quoting D.C. Circuit Judge Katsas, sitting by designation on an Eleventh Circuit panel, Justice Kavanaugh reiterated that "[a]s Judge Katsas has rightly stated, 'we cannot treat an injury as "concrete" for Article III purposes based only on Congress's say-so.' " *TransUnion*, 141 S. Ct. at 2205, *quoting Trichell v. Midland Credit Management, Inc*., 964 F.3d 990, 999 n.2 (11th Cir. 2020). Justice Kavanaugh elaborated:

> To appreciate how the Article III "concrete harm" principle operates in practice, consider two different hypothetical plaintiffs. Suppose first that a Maine citizen's land is polluted by a nearby factory. She sues the company, alleging that it violated a federal environmental law and damaged her property. Suppose also that a second plaintiff in Hawaii files a federal lawsuit alleging that the same company in Maine violated that same environmental law by polluting land in Maine. The violation did not personally harm the plaintiff in Hawaii.
>
> Even if Congress affords both hypothetical plaintiffs a cause of action (with statutory damages available) to sue over the defendant's legal violation, Article III standing doctrine sharply distinguishes between those two scenarios. The first lawsuit may of course proceed in federal court because the plaintiff has suffered concrete harm to her property. But the second lawsuit may not proceed because that plaintiff has not suffered any physical, monetary, or cognizable

"[e]very class member must have Article III standing in order to recover individual damages."[206] The Court declined to address whether every class member must demonstrate standing before a court certifies a class,[207] but plainly the prospect that, as in *Ramirez,* the majority of a proposed class is determined not to have standing following trial on the merits has implications for typicality, adequacy of representation, predominance. manageability, and the definition of a proposed class, among other issues that courts must grapple with under Federal Rule of Civil Procedure 23 in ruling on motions for class certification.[208] Since standing may be raised at any time during the litigation, and must exist at

---

> intangible harm traditionally recognized as providing a basis for a lawsuit in American courts. An uninjured plaintiff who sues in those circumstances is, by definition, not seeking to remedy any harm to herself but instead is merely seeking to ensure a defendant's "compliance with regulatory law" (and, of course, to obtain some money via the statutory damages). *Spokeo*, 578 U. S., at 345 (THOMAS, J., concurring) (internal quotation marks omitted); *see Steel Co.*, 523 U.S., at 106–107. Those are not grounds for Article III standing.
>
> As those examples illustrate, if the law of Article III did not require plaintiffs to demonstrate a "concrete harm," Congress could authorize virtually any citizen to bring a statutory damages suit against virtually any defendant who violated virtually any federal law. Such an expansive understanding of Article III would flout constitutional text, history, and precedent. In our view, the public interest that private entities comply with the law cannot "be converted into an individual right by a statute that denominates it as such, and that permits all citizens (or, for that matter, a subclass of citizens who suffer no distinctive concrete harm) to sue." *Lujan*, 504 U.S., at 576–577.

TransUnion, 141 S. Ct. at 2205-06 (footnotes omitted). With respect to the requirement that an injury be both concrete *and* particularized, Justice Kavanaugh observed that

> if there were no concrete-harm requirement, the requirement of a particularized injury would do little or nothing to constrain Congress from freely creating causes of action for vast classes of unharmed plaintiffs to sue any defendants who violate any federal law. (Congress might, for example, provide that everyone has an individual right to clean air and can sue any defendant who violates any air-pollution law.) That is one reason why the Court has been careful to emphasize that concreteness and particularization are separate requirements.

Id. 2206 n.2.

[206] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2208 (2021).

[207] *See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2208 n.4 (2021).

[208] *See generally infra* § 27.07[3] (class certification in data breach putative class action suits); *supra* § 25.07[2] (class certification generally, in Internet and mobile litigation). *Ramirez* was reversed and remanded without consideration of whether his claims were typical of those of class members under Rule 23. *See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2214 (2021).

all times,[209] and for all claims[210] and for each form of relief sought,[211] standing may play an even greater role in class certification decisions in cybersecurity breach putative class action suits premised on the risk of future harm than it had prior to *Ramirez*.

TransUnion v. Ramirez also is relevant to standing determinations at the outset of a putative data breach class action suit, even though the evidence required to establish standing will be less exacting than it was in *Ramirez,* which was decided following trial. Assuming as true plaintiffs' allegation that TransUnion violated the Fair Credit Reporting Act's requirement to use reasonable procedures in internally maintaining class members' credit files,[212] the Supreme Court held that only those class members whose information was

---

[209]*See, e.g.*, *Uzuegbunam v. Preczewski,* 141 S. Ct. 792, 796 (2021).

[210]*See, e.g.*, *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2208 (2021). As Justice Kavanaugh explained,

> plaintiffs bear the burden of demonstrating that they have standing. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Every class member must have Article III standing in order to recover individual damages. "Article III does not give federal courts the power to order relief to any uninjured plaintiff, class action or not." *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 466 (2016) (ROBERTS, C. J., concurring). Plaintiffs must maintain their personal interest in the dispute at all stages of litigation. *Davis v. Federal Election Comm'n*, 554 U.S. 724, 733 (2008). A plaintiff must demonstrate standing "with the manner and degree of evidence required at the successive stages of the litigation." *Lujan*, 504 U.S., at 561, 112 S.Ct. 2130. Therefore, in a case like this that proceeds to trial, the specific facts set forth by the plaintiff to support standing "must be supported adequately by the evidence adduced at trial." *Ibid*. (internal quotation marks omitted). And standing is not dispensed in gross; rather, plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages). *Davis*, 554 U.S., at 734; *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc*., 528 U.S. 167, 185 (2000).

TransUnion LLC v. Ramirez, 141 S. Ct. at 2207-08 (footnote omitted).

[211]*See, e.g., TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210 (2021), *quoting Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc*., 528 U.S. 167, 185 (2000).

[212]The Supreme Court noted, without deciding, that at least one circuit had held that there is no FCRA violation where information is not disseminated to third parties. *See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2221 n.5 (2021), *citing Washington v. CSC Credit Servs. Inc*., 199 F.3d 263, 267 (5th Cir. 2000) ("In light of the purposes of the FCRA, we find that the actionable harm the FCRA envisions is improper disclosure, not the mere risk of improper disclosure that arises when "reasonable procedures" are not followed and disclosures are made. Accordingly, a plaintiff bringing a claim that a reporting agency violated the 'reasonable procedures' requirement of § 1681e must first show that the reporting agency released the report in violation of § 1681b."). *But see, e.g., Beaudry*

provided to third parties had standing—reasoning that the harm from being labeled a "potential terrorist" bore "a sufficiently close relationship" to the harm caused by false and defamatory statements.[213] The remaining 6,332 class members—whose designation as potential terrorists in OFAC alerts had *not* been communicated to potential creditors—did not have Article III standing. Justice Kavanaugh—again analogizing the case to a suit for defamation for purposes of evaluating whether plaintiffs had suffered a concrete injury—explained that publication was essential to liability in a suit for defamation and that there was no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounted to a concrete injury.[214] Justice Kavanaugh wrote that "where allegedly inaccurate or misleading information sits in a company database, the plaintiffs' harm is roughly the same, legally speaking, as if someone wrote a defamatory letter and then stored it in her desk drawer. A letter that is not sent does not harm anyone, no matter how insulting the letter is."[215] The Court reiterated that "[t]he mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm."[216] The same undoubtedly could be said for many security breaches where information potentially may have been exposed but there is no reason to believe it has or will be used for financial fraud or identity theft.

In *Ramirez,* plaintiffs also argued that they had standing based on the risk of future harm because the existence of misleading OFAC alerts in their internal credit files allegedly exposed them to a material risk that the information would be disseminated in the future to third parties and thereby cause them harm. The Supreme Court, however, distinguished suits for damages from suits for injunctive relief, emphasizing that *Clapper* was a suit for injunctive relief. Justice Kavanaugh explained that "a person exposed

---

v. TeleCheck Services, Inc., 579 F.3d 702. 707-08 (6th Cir. 2009) (criticizing *CSC Credit* as based on a pre-1996 version of the statute, that was subsequently amended).

[213]*See TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2209 (2021).

[214]*See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2209 (2021), *citing Owner-Operator Independent Drivers Assn., Inc. v. U.S. Dept. of Transportation,* 879 F.3d 339, 344-45 (D.C. Cir. 2018).

[215]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210 (2021).

[216]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210 (2021).

to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial."[217] However, "a plaintiff 's standing to seek injunctive relief does not necessarily mean that the plaintiff has standing to seek retrospective damages."[218] The Supreme Court agreed with TransUnion's argument that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm."[219] In language reminiscent of the Third Circuit's analysis of standing in data breach putative class action suits in *Reilly v. Ceridian Corp*.[220] (as discussed earlier in this section), Justice Kavanaugh cited TransUnion's "persuasive argument" that

> if an individual is exposed to a risk of future harm, time will eventually reveal whether the risk materializes in the form of actual harm. If the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages. If the risk of future harm does not materialize, then the individual cannot establish a concrete harm sufficient for standing . . . .[221]

As Justice Kavanaugh observed, "there is a significant difference between (i) an actual harm that has occurred but is not readily quantifiable, as in cases of libel and slander *per*

---

[217]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210 (2021), *citing Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 414 n.5 (2013); and *Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983).

[218]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210 (2021).

[219]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2210-11 (2021) (emphasis in original).

[220]*Reilly v. Ceridian Corp*., 664 F.3d 38, 41-46 (3d Cir. 2011). *Reilly* is discussed earlier in this section 27.07[2][B] and in section 27.07[2][A].

[221]*TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2211 (2021). Justice Kavanaugh offered the following analogy:

> Suppose that a woman drives home from work a quarter mile ahead of a reckless driver who is dangerously swerving across lanes. The reckless driver has exposed the woman to a risk of future harm, but the risk does not materialize and the woman makes it home safely. . . . [T]hat would ordinarily be cause for celebration, not a lawsuit. . . . But if the reckless driver crashes into the woman's car, the situation would be different, and (assuming a cause of action) the woman could sue the driver for damages.

Id. The Court expressed no position on whether or how an emotional or psychological harm could suffice for Article III purposes—for example, by analogy to the tort of intentional infliction of emotional distress. *See id.* n.7.

se, and (ii) a mere risk of future harm."[222] The mere risk of future harm, without more, is insufficient to demonstrate Article III standing in a suit for damages.

This aspect of the Court's analysis in *Ramirez* also is likely to impact standing determinations in cybersecurity breach putative class action suits.

In fact, many people have their information exposed without becoming victims of identity theft. Cybersecurity attacks occur for myriad reasons unrelated to consumer fraud. Indeed, according to the Ponemon Institute 47% of data breaches in 2020 were not motivated by financial interests. Among other things, 13% of data breaches in 2020 where initiated by state actors seeking information about the United States and 13% were undertaken by hacktivists, for the perceived fun and challenge of doing so or for policy or political objectives[223] (including an attack on Capital One Bank, which was not motivated by financial objectives[224]). Attacks may also be undertaken by state actors that are not seeking to use personal information for financial fraud. In fact, one of the more significant attacks uncovered in early 2021 by Google's Project Zero was a 9 month counterterrorism operation by a U.S. ally.[225]

Even where information is sought to be used for financial harm, the thieves may be unsuccessful depending on what information was taken and how quickly it was uncovered. For example, stolen credit card numbers can't be used for identity theft and credit card companies often cancel cards quickly, before consumers could be impacted. Moreover, consumers themselves can put credit freezes on their accounts to substantially reduce the risk of identity theft.

Similarly, if data accessed was protected by strong encryp-

---

[222] *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190, 2211 (2021).

[223] *See* IBM Security & Ponemon Institute, *Cost of a Data Breach Report 2020* 38, *available at* https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (click "See the report and calculator").

[224] *See* Lardieri, Alexa, *Hacker Accessed Personal Information of 100m Capital One Customers*, USNews (July 30, 2019) ("Capital One does not believe the information was used for fraud or disseminated"), *available at* https://www.usnews.com/news/national-news/articles/2019-07-30/hacker-accesses-personal-information-of-100m-capital-one-customers

[225] *See* Patrick Howell O'Neill, *Google's top security teams unilaterally shut down a counterterrorism operation*, MIT Technology Review, Mar. 26, 2021; Chris Smith, *A massive hack that Google thwarted was actually a counterterrorism operation,* BGR, Mar. 28, 2021.

tion or hashed and salted, a person accessing it may be unable to do anything with it.

Usernames and passwords, without more, may not subject users to a risk of harm if they access website or mobile accounts where financial information is not collected or stored, provided users do not use the same username/password combination for financial accounts.

Many cyber attackers are opportunistic, taking whatever information is available, rather than targeting a specific user base for financial harm.

Yet, even where thieves target specific information, simply acquiring it is not the same as being able to use it—especially if 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 is flawed, and has been expressly rejected by the Fourth Circuit. More fundamentally, the Second, Fourth, Eighth and Eleventh Circuits expressly hold, consistent with *Clapper* and *TransUnion*, 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.[226] Providing credit monitoring services to allay customer concerns is not, and should not be viewed as, an admission that a breach was severe.

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, Eighth and Eleventh Circuits (and the Second Circuit in a nonprecedential opinion).

---

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

In addition to circuit courts, a number of district courts have dismissed security breach cases for lack of standing, on various grounds, since *Spokeo*.[227]

---

[227]*See, e.g.*, *Browne v. US Fertility LLC,* Civil Action No. 21-367, 2021 WL 2550643, at *2-3 (E.D. Pa. June 22, 2021) (following *Reilly* in dismissing plaintiff's putative class action suit arising out of the theft of patient personal information from Shady Grove Fertility clinics in Pennsylvania, Maryland, and New Jersey, holding that Browne's expenditure of $181.27 to purchase LifeLock services did not establish injury-in-fact and that he could "not achieve standing on the allegation that Defendants breached an implied contract or were unjustly enriched."); *Graham v. Universal Health Service, Inc.*, Civil Action No. 20-5375, 2021 WL 1962865, at *3-5 (E.D. Pa. May 17, 2021) (dismissing plaintiffs' putative class claims for negligence, breach of implied contract, breach of fiduciary duty, and breach of confidence, arising out of a ransomware attack, for those plaintiffs whose injuries were premised on future risks and preventative measures, while denying defendant's motion to dismiss brought by the one plaintiff who alleged that his insurance premiums were increased as a result of the attack; "The target of a ransomware attack is the holder of the confidential data; the misappropriation of the data, whether by theft or merely limitation on access to it, is generally the means to an end: extorting payment. A court is still left to speculate, as in *Reilly*, whether the hackers acquired Plaintiffs' PHI in a form that would allow them to make unauthorized transactions in their names, as well as whether Plaintiffs are also intended targets of the hackers' future criminal acts."); *Springmeyer v. Marriott International, Inc*., Case No. 20-cv-867-PWG, 2021 WL 809894, at *3-4 (D. Md. Mar. 3, 2021) (dismissing plaintiffs' putative cybersecurity breach class action with prejudice where plaintiffs could not allege facts to show injuries fairly traceable to Marriott's alleged conduct; "mere repetition of conclusory and nonspecific allegations of Marriott's alleged shortcomings does not overcome the need to plead sufficient facts relating to what it did or did not do that led to the injuries claimed by the Plaintiffs. What is missing are any alleged facts to support these conclusory statements. For example, Plaintiffs do not allege any facts about what measures Marriott did or did not take to protect PII, what alleged inadequacies in its systems it should have disclosed, what 'standard and reasonably available steps' existed that Marriott did not take, how Marriott failed to detect the data breach, or why it did not provide timely and accurate notice of the breach."); *Clemens v. ExecuPharm, Inc.*, Civil Action No. 20-3383, 2021 WL 735728, at *3-5 (E.D. Pa. Feb. 25, 2021) (following *Reilly* in dismissing plaintiff's claims arising out of a ransomware attack undertaken by CLOP, for lack of standing, where plaintiff, a former employee, had her information (including her Social Security number, banking information (a copy of a personal check for direct deposit), driver's license, date of birth, home address, spouse's name, beneficiary information (including Social Security numbers) and payroll tax forms (such as W-2 and W-4)) stolen and released on the dark web, which she had argued evidenced that harm was certainly impending, despite alleging that she experienced actual harm from her time, money and effort to protect her information based on the imminent risks she allegedly faced, and that she alleged harm to her private contract

rights); *Rahman v. Marriott International, Inc.*, Case No. SA CV 20-00654-DOC-KES, 2021 WL 346421 (C.D. Cal. Jan. 12, 2021) (dismissing plaintiff's complaint under the California Consumer Privacy Act and for breach of contract, breach of implied contract, unjust enrichment and unfair competition, for lack of Article III standing, in a suit arising out of Russian employees accessing putative class members' names, addresses, and other publicly available information, because the sensitivity of personal information, combined with its theft, are prerequisites to finding that a plaintiff adequately alleged injury in fact); *In re Rutter's Inc. Data Security Breach Litigation*, 511 F. Supp. 3d 514 (M.D. Pa. 2021) (applying *Reilly* in holding that plaintiffs could not establish standing where their credit card information had been exposed but they had not incurred any loss; "As in *Reilly*, the harm that Plaintiffs . . . may face in the future—even if that harm is arguably more likely to occur than in *Reilly*—depends on multiple levels of impermissible speculation. To hold here that a plaintiff in a data breach class action, who has presently suffered no cognizable injury, can establish standing with allegations that she suffers some unquantifiable risk of future harm based on the lone fact that other people were harmed would totally undermine *Reilly*'s bright-line rule."); *Hartigan v. Macy's, Inc*., 501 F. Supp. 3d 1 (D. Mass. 2020) (dismissing putative class action claims premised on future harm, arising out of a data breach, for lack of Article III standing); *Stasi v. Inmediata Health Group Corp*., Case No.: 19cv2353 JM (LL), 2020 WL 2126317, at *4-10 (S.D. Cal. May 5, 2020) (dismissing plaintiffs' claims for negligence, negligence *per se*, breach of contract, violation of California's Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 to 56.37, and violation of the Minnesota Health Records Act, Minn. Stat. Ann. §§ 144.291 to 144.34, in a putative security breach class action suit arising out of a breach exposing medical records, for lack of Article III standing, where the type of information exposed, and resulting risk of identity theft, did not rise to a level sufficient to confer standing, where plaintiff did not allege that personal information was stolen or hacked, but merely made accessible via the Internet temporarily, and plaintiffs' information allegedly exposed did not include Social Security numbers or financial information); *Brett v. Brooks Bros. Group,* No. CV 17-4309-DMG (Ex), 2018 WL 8806668, at *4 (C.D. Cal. Sept. 6, 2018) (dismissing plaintiffs' claims for breach of implied contract, negligence, unlawful business practices under the California Unfair Competition Law, unfair business practices under the UCL, fraudulent/deceptive business practices under the UCL, and breach of covenant of good faith and fair dealing, in a putative data breach class action suit, for lack of Article III standing, where hackers allegedly stole plaintiffs' names, credit and debit card numbers (along with card expiration dates and verification codes) and possibly the Brooks Brothers store zip codes where plaintiffs made purchases as well as the time of those purchases, because "[t]his information simply does not rise to the level of sensitivity of the information in *Krottner* and *Zappos* or similar cases[;]" and dismissing plaintiffs' claim for an alleged violation of California's security breach notification law for lack of standing, premised on Brooks Brothers' disclosure about monitoring account statements, as required by California's security breach notification law, Cal. Civ. Code § 1798.82(d)(1), because "The Court will not interpret bare statutory compliance as an af-

27.07[3] Substantive Claims, Causation, Proof of Harm and Class Certification

Even where standing is established, plaintiffs in data breach putative class action suits may have difficulty prevailing because of the difficulties associated with establishing causation and injury or harm (or damages) in most cases, which in turn may make it difficult for plaintiffs to obtain class certification. 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[1] or federal appellate[2] and district[3] courts. While a

---

firmative admission of imminent future harm. Indeed, such an interpretation would require courts to conclude that a data breach's mere occurrence establishes imminent risk of future harm, which is contrary to controlling Article III precedent, and it would perversely incentivize companies to provide vague or misleading disclaimers to customers affected by a data breach in an attempt to avoid litigation."); *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 (1) allegedly 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 alleged that fake tax returns were submitted in plaintiff's name and a fraudulent account opened, because those injuries could not have been caused by the breach of social security, bank account, and routing numbers); *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.").

[Section 27.07[3]]

[1]*See, e.g., Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702,

company may have a contractual claim against a third party

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 allegedly 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).

[2]*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 retaining certain credit card information); *In re SuperValu, Inc., Customer Data Security Breach Litig.*, 925 F.3d 955, 964-66 (8th Cir. 2019) (affirming dismissal of plaintiff's consumer protection claims under the Illinois Consumer Fraud and Deceptive Business Practices Act, the Illinois Personal Information Protection Act, and the Illinois Uniform Deceptive Trade Practices Act, where his alleged injuries—time spent monitoring his account, a single fraudulent charge to his credit card, and the effort expended replacing the card—did not constitute actual damages); *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 817-18 (7th Cir. 2018) (affirming dismissal, under Illinois and Missouri law, of the banks' putative class action suit against merchants, where the economic loss rule barred plaintiffs' tort claims (and Illinois law did not impose on retailers a special relationship with customers that obligated them to protect financial information from hackers), 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); *In re SuperValu, Inc.*, 925 F.3d 955, 962-66 (8th Cir. 2019) (affirming dismissal of claims for negligence, finding no special relationship between vendor and customer and holding that plaintiff could not premise a negligence claim on an alleged violation of the Federal Trade Commission Act, which does not provide for a private right of action, under various Illinois consumer protection and privacy statutes, and for breach of implied contract and unjust enrichment); *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613, 614-15 (9th Cir. 2021) (affirming dismissal of claims for negligence, breach of implied contract, negligent misrepresentation, and violation of Nev. Rev. Stat. Ann. § 41.600 (deceptive practices), in a suit arising out of a data breach, because (1) lost time was not a cognizable injury for the purpose of establishing compensable damages (at least absent out of pocket expenses), (2) emotional distress was not compensable under Nevada law because, in the absence of physical impact, proof of serious emotional distress causing physical injury or illness must be presented, and (3) plaintiff's claim for diminution in the alleged value of her personal information was not compensable under Nevada law as unduly speculative); *Stollenwerk v. Tri–West Health Care Alliance*, 254 F. App'x 664, 666–68

vendor responsible for a security breach, consumer contracts

(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).

[3]*See, e.g.*, *Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *3-6 (N.D. Cal. July 28, 2021) (dismissing with prejudice, for failing to adequately allege injury, plaintiff's negligence, breach of contract, and California unfair competition claims based on amended allegations of loss of value of PII (where plaintiff did not allege that he had been unable to sell, profit from, or monetize his personal information and the court inferred that an expired credit card in any case had no value), risk of future harm (where plaintiff alleged he canceled the credit cards associated with the breach and that those cards had expired), out of pocket expenses and lost time (where plaintiff failed to allege that credit monitoring services were "reasonable and necessary"), and benefit of the bargain); *Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *3-7 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's claims for negligence, breach of contract and violations of the California unfair competition law for failure to plead cognizable injury, in a cybersecurity breach putative class action suit; rejecting arguments based on loss of the value of plaintiff's PII, future risk of identity theft, out-of-pocket expenses for credit monitoring services and loss of the benefit of the bargain); *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 "identifiable 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

rarely provide such assurances and individuals usually are not intended beneficiaries of corporate security contracts with outside vendors.[4] Some representations to consumers about a company's security practices also may be viewed as merely puffery.[5]

---

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 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).

[4]*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 Global 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).

[5]*See, e.g.*, *In re Yahoo! Inc. Customer Data Security Breach Litiga-*

The level of injury that suffices to establish Article III standing may not be sufficient to constitute damages under an array of state laws where damage or injury is an element of the claim.[6] Thus, many common law and other claims in

---

tion, No. 16-MD-02752-LHK, 2017 WL 3727318, at *26 (N.D. Cal. Aug. 30, 2017) (holding that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust" was non-actionable puffery under California's unfair competition statute because the statement was vague and an "all-but-meaningless superlative[,]"and said "nothing about the specific characteristics" of the products or services offered by the defendant, and thus could not have been relied upon by a reasonable consumer); *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."); *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566, 592 (S.D. Tex. 2011) (dismissing 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 upon by plaintiffs; holding that slogans such as *The Highest Standards and The Most Trusted Transactions* were puffery on which the financial institution plaintiffs could not reasonably rely), *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).

These cases and puffery claims in data breach cases are addressed in greater detail at the end of this section 27.07[3].

[6] *See, e.g.*, *Pruchnicki v. Envision Healthcare Corp.,* 845 F. App'x 613, 614-15 (9th Cir. 2021) (affirming dismissal of claims for negligence, breach of implied contract, negligent misrepresentation, and violation of Nev. Rev. Stat. Ann. § 41.600 (deceptive practices), in a suit arising out of a data breach, because (1) lost time was not a cognizable injury for the purpose of establishing compensable damages (at least absent out of pocket expenses) and (2) plaintiff's claim for diminution in the alleged value of her personal information was not compensable under Nevada law as unduly speculative, even though she was found to have Article III standing); *Krottner v. Starbucks Corp.,* 406 F. App'x 129, 131 (9th Cir. 2010) (reiterating that the same appellate panel's "holding that Plaintiffs-Appellants pled an injury-in-fact for purposes of Article III standing [in a security breach case] does not establish that they adequately pled damages for purposes of their state-law claims."), *citing Doe v. Chao*, 540 U.S. 614,

data breach cases may be dismissed where the plaintiff cannot plead or prove damage.

Causation likewise may be a difficult hurdle for a plaintiff to surmount in data breach case if the plaintiff has been subject to multiple breaches.[7]

624–25 (2004) (explaining that an individual may suffer Article III injury and yet fail to plead a proper cause of action); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *5 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's claims in a data breach putative class action suit; "the allegations required to sufficiently plead injury-in-fact for purposes of Article III standing are not the same as those required to plead damages for purposes of state law claims."); *Ruiz v. Gap, Inc*., 622 F. Supp. 2d 908, 913-14 (N.D. Cal. 2009) (granting summary judgment for the defendant on plaintiff's negligence claim in a security breach case brought by a job applicant whose personal information had been stored on a laptop of the defendant's that had been stolen, because 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; "While Ruiz has standing to sue based on his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law."), *aff'd mem.*, 380 F. App'x 689 (9th Cir. 2010).

[7] *See, e.g.*, *Katz v. Pershing, LLC*, 672 F.3d 64, 75 (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 plaintiff could not state a claim for negligence in the absence of causation and harm); *Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016) (rejecting negligence claims for lack of causation because plaintiff had been the subject of a "previous, unrelated data breach"); *Fu v. Wells Fargo Home Mortgage*, Civil Action No. 2:13–cv–01271–AKK, 2014 WL 4681543, at *4-5 (N.D. Ala. Sept. 12, 2014) (granting summary judgment for the defendant on plaintiff's negligence claim for lack of causation where identity theft had "multiple possible causes" yet plaintiff failed to "provide[] sufficient evidence . . . that the unsecured email led to the [identity] theft," as opposed to "other possible theories" including that the thief "obtained [plaintiff's] personal information from sources other than the email"); *Gardner v. Health Net, Inc*., No. CV 10-2140 PA (CWX), 2010 WL 11571242, at *2 (C.D. Cal. Nov. 29, 2010) (dismissing with prejudice plaintiffs' negligence claim for lack of causation and damage, where they had alleged that they suffered damages in the form of "expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; and time spent initiating fraud alerts."); *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

One of the most commonly asserted claims in a cybersecurity breach putative class action suit is negligence. Like many common law claims, however, a claim for negligence will not be viable if a plaintiff cannot allege damage.[8]

---

causation); *Jones v. Commerce Bank, N.A.*, No. 06 Civ. 835(HB), 2007 WL 672091, at *4 (S.D.N.Y. Mar. 6, 2007) (granting summary judgment for the defendant on plaintiff's negligence claim based on identity theft because "[t]he thieves might well have stolen Plaintiff's information without any negligence on the part of [defendant]").

Individualized issues of causation also may make it difficult for a plaintiff to obtain class certification in a cybersecurity breach case, as discussed later in this section 27.07[3]. *See, e.g.*, *McGlenn v. Driveline Retail Merchandising, Inc.*, No. 18-cv-2097, 2021 WL 165121, at *8-10 (C.D. Ill. Jan. 19, 2021) (denying class certification in a data breach case where a Payroll Department employee of the defendant responded to a phishing scam by sending 15,878 2016 W-2 forms to a scammer posing as Driveline's CFO, which contained sensitive personally identifiable information (PII), including names, mailing addresses, Social Security numbers, and wage and withholding information, for lack of commonality due to individualized issues of causation, injury and damage).

[8] *See, e.g.*, *Pruchnicki v. Envision Healthcare Corp.,* 845 F. App'x 613, 614-15 (9th Cir. 2021) (affirming dismissal of claims for negligence, breach of implied contract, negligent misrepresentation, and violation of Nev. Rev. Stat. Ann. § 41.600 (deceptive practices), in a suit arising out of a data breach, because (1) lost time was not a cognizable injury for the purpose of establishing compensable damages (at least absent out of pocket expenses), (2) emotional distress was not compensable under Nevada law because, in the absence of physical impact, proof of serious emotional distress causing physical injury or illness must be presented, and (3) plaintiff's claim for diminution in the alleged value of her personal information was not compensable under Nevada law as unduly speculative); *Krottner v. Starbucks*, 406 F. App'x 129, 131 (9th Cir. 2010) (affirming dismissal of plaintiffs' negligence claim, arising out of the theft of a laptop containing their personal data, where plaintiff could not allege damages); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *3-6 (N.D. Cal. July 28, 2021) (dismissing with prejudice, for failure to adequately allege injury, plaintiff's negligence, breach of contract, and California unfair competition claims based on amended allegations of loss of value of PII (applying *Pruchnicki* to a claim brought under California law, where plaintiff did not allege that he had been unable to sell, profit from, or monetize his personal information and the court inferred that an expired credit card in any case had no value), risk of future harm (where plaintiff alleged he canceled the credit cards associated with the breach and that those cards had expired), out of pocket expenses and lost time (where plaintiff failed to allege that credit monitoring services were "reasonable and necessary"), and benefit of the bargain); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *3-5 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's claims for negligence, breach of contract, and violations of California's unfair competition law, in a data breach putative class action suit, for failure to plead a cognizable injury

Negligence claims likewise often fail, both in state[9] and federal[10] court, based on the economic loss rule (referred to

---

by alleging the future risk of identity theft, the loss of value of his PII, out of pocket expenses for credit monitoring, and the benefit of the bargain); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2020 WL 7408230, at *6 (N.D. Cal. June 1, 2020) (dismissing in part plaintiffs' claims for negligence, in a putative cybersecurity class action suit, to the extent based on lost personal information and the risk of future harm, as "not sufficient to sustain a negligence claim under California law as they are speculative, not appreciable, and not present."); *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 963 (S.D. Cal. 2014) (dismissing plaintiffs' negligence claim in a putative security breach class action suit; "without specific factual statements that Plaintiffs' Personal Information has been misused, in the form of an open bank account, or un-reimbursed charges, the mere 'danger of future harm, unaccompanied by present damage, will not support a negligence action.' "); *Gardner v. Health Net, Inc.*, No. CV 10-2140 PA (CWX), 2010 WL 11571242, at *2 (C.D. Cal. Nov. 29, 2010) (dismissing with prejudice plaintiffs' negligence claim for lack of causation and damage, where they had alleged that they suffered damages in the form of "expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; and time spent initiating fraud alerts."); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1054 (E.D. Mo. 2009) (dismissing plaintiff's negligence claim, arising out of an alleged database security breach, because the increased risk of identity theft, the time spent to monitor credit and other accounts, the loss and compromise of plaintiff's personal information, the loss of exclusive control over this information, and the invasion of his privacy, causing him to spend significant amounts of time monitoring his credit and medical information, were insufficient to state a claim under Missouri law); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913-14 (N.D. Cal. 2009) (granting summary judgment for the defendant on plaintiff's negligence claim in a security breach case brought by a job applicant whose personal information had been stored on a laptop of the defendant's that had been stolen, because 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; "Under California law, the breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action for negligence. . . . While Ruiz has standing to sue based on his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law."), *aff'd mem.*, 380 F. App'x 689 (9th Cir. 2010).

[9] *See, e.g.*, *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 455 Mass. 458, 469-70, 918 N.E.2d 36, 46-47 (Mass. 2009) (affirming dismissal of negligence claims as barred by the economic loss rule, holding that the costs of replacing credit cards for compromised accounts were economic losses).

[10] *See, e.g.*, *In re TJX Cos. Retail Security Breach Litigation*, 564 F.3d 489, 498–99 (1st Cir. 2009) (affirming dismissal of negligence claims under

Massachusetts law in a data breach case brought by banks that had issued credit and debit cards to customers, who subsequently had their credit and debit card information stolen from defendant's computers, based on the economic loss doctrine); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 177–78 (3d Cir. 2008) (affirming dismissal of Sovereign Bank's negligence claim under Pennsylvania law based on the economic loss doctrine, in a case arising out of data breach); *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 817-18 (7th Cir. 2018) (holding, under Illinois and Missouri law, that the economic loss rule barred issuing banks' tort claims against a retail merchant arising from the merchant's failure to adopt adequate security measures to prevent a data breach that resulted in the disclosure of information about the banks' customers' use of their credit and debit cards, even though there was no direct contract between the banks and the merchant, where the merchant assumed contractual data security responsibilities in joining the credit card networks, and all parties in the card networks expected other parties to comply with industry-standard data security policies as matter of contractual obligation); *In re SuperValu, Inc*., 925 F.3d 955, 962-64 (8th Cir. 2019) (affirming dismissal of claims for negligence, finding no special relationship between vendor and customer and holding that plaintiff could not premise a negligence claim on an alleged violation of the Federal Trade Commission Act, which does not provide for a private right of action; "In Illinois, generally there is no affirmative duty to protect another from a criminal attack unless one of four historically recognized 'special relationships' exists between the parties. . . . The failure of Illinois law to impose this type of common-law duty on merchants mandates dismissal of Holmes's negligence claim."); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *6 (N.D. Cal. July 28, 2021) (dismissing with prejudice plaintiff's negligence claim where plaintiff was in privity of contract for the sale of goods with defendant and could not allege a special relationship); *Finesse Express, LLC v. Total Quality Logistics, LLC*, Case No. 1:20cv235, 2021 WL 1192521, at *6-7 (S.D. Ohio Mar. 31, 2021) (dismissing Ohio negligence claim in a putative security breach class action suit arising out of a hacker gaining access to the defendant freight broker's IT system, which compromised tax ID, bank account and invoice information); *In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1038-40 (N.D. Cal. 2021) (dismissing, in a putative class action suit, plaintiffs' California negligence claim alleging that Zoom failed to protect the security of its platform against breaches referred to as "Zoombombing," which allegedly exposed users to harmful material, based on the economic loss rule); *Bray v. Gamestop Corp*., 1:17-cv-1365, 2018 WL 11226516, at *4 (D. Del. Mar. 16, 2018) (dismissing plaintiffs' negligence and negligence *per se* claims, based on the economic loss doctrine, in a putative data breach class action suit); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc*., Case No.: 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016) (dismissing plaintiff's negligence claim premised on a credit card being compromised in a data breach, as barred by the economic loss doctrine); *Castillo v. Seagate Technology, LLC*, Case No. 16-cv-01958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016) (dismissing plaintiffs' negligence claims arising out of a security breach based on the economic loss rule where a special

in some cases as a doctrine), which holds that purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage. The economic loss rule requires a plaintiff to recover in contract for purely economic loss due to disappointed expectations, not tort, unless the plaintiff can demonstrate harm above and beyond a broken contractual promise.[11] In cybersecurity breach cases, it "bars a plaintiff from recovering for purely economic losses under a tort theory of negligence."[12]

"The purpose of the economic loss rule is to 'prevent[ ] the law of contract and the law of tort from dissolving one into the other.' "[13] It reflects the belief "that tort law affords the proper remedy for loss arising from personal injury or dam-

---

relationship could not be shown); *In re Target Corp. Data Security Breach Litigation*, 66 F. Supp. 3d 1154, 1171-76 (D. Minn. 2014) (dismissing negligence claims under Alaska, California, Illinois, Iowa, and Massachusetts law, in a cybersecurity breach putative class action suit, based on the economic loss rule); *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 967 (S.D. Cal. 2014) (dismissing negligence claims in a data security breach case, based on the economic loss rule, under California law); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528-30 (N.D. Ill. 2011) (applying Illinois law in dismissing negligence claims in a data breach case based on the economic loss rule); *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, at *21-25 (S.D. Tex. Mar. 31, 2011) (dismissing with prejudice financial institution plaintiffs' negligence claims against credit card processor defendants under New Jersey, Texas and Ohio law, based on the economic loss doctrine); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (dismissing plaintiff's negligent misrepresentation claim under the economic loss doctrine in a putative class action suit involving the alleged disclosure of plaintiff's email address and the potential dissemination of certain personal information from her Emigrant Bank account).

[11] *Robinson Helicopter Co. v. Dana Corp.,* 34 Cal. 4th 979, 988, 22 Cal. Rptr. 3d 352, 358 (2004).

[12] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011).

[13] *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 453 (N.D. Cal. 2018), *quoting Robinson Helicopter Co. v. Dana Corp*., 34 Cal. 4th 979, 988, 22 Cal. Rptr. 3d 352, 273 (2004) (quoting *Rich Products Corp. v. Kemutec, Inc*., 66 F. Supp. 2d 937, 969 (E.D. Wis. 1999)). In *In re Apple*, the court held that the economic loss doctrine does not apply to civil claims under the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030, because a CFAA claim "is decidedly not a state-law tort claim but is instead a federal claim appended to a federal criminal statute." 347 F. Supp. 3d at 453.

ages to one's property, whereas contract law and the Uniform Commercial Code provide the appropriate remedy for economic loss stemming from diminished commercial expectations without related injury to person or property."[14] A minority of states recognize an independent duty exception to the economic loss rule in narrow special circumstances typically inapplicable to security breach cases,[15] although district

---

[14]*In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011).

[15]*See, e.g.*, *In re Target Corp. Data Security Breach Litigation*, 66 F. Supp. 3d 1154, 1171-76 (D. Minn. 2014) (surveying and summarizing case law on this issue in a number of jurisdictions, finding the independent duty exception inapplicable to plaintiffs suing under Alaska, California, Illinois, Iowa, and Massachusetts law, in a cybersecurity breach putative class action suit). *But see 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 because (1) the Issuer Banks constituted an "identifiable 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"); *Dittman v. UPMC*, 196 A.3d 1036 (Pa. 2018) (holding that the claims of employees for economic harm arising out of a security breach were not barred by the economic loss rule under Pennsylvania law because 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); *see also, e.g.*, *Sweet v. BJC Health System*, Case No. 3:20-CV-00947-NJR, 2021 WL 2661569, at *8 (S.D. Ill. June 29, 2021) (denying defendant's motion to dismiss tort claims; "In most data breach cases, the relationship between plaintiffs and defendants is purely commercial, the relationship between a business and a customer. Here, however, Defendants are health care providers, and Plaintiffs are their patients. There are both statutory obligations and common law duties which Defendants owe to their patients, which may overlap and may also diverge from their contractual obligations . . . [and] provide an independent basis for tort liability, and dismissal is thus not warranted under the economic loss doctrine at this time."); *In re Wawa, Inc. Data Security Litigation*, Civil Action No. 19-6019, 2021 WL 1818494, at *2-7 (E.D. Pa. May 6, 2021) (applying *Dittman v. UPMC* to allow financial institution plaintiffs to proceed with their claim of negligence "based on their allegations that Wawa violated a duty to protect sensitive payment card information that was independent of any potential contractual relationship that existed.").

courts, construing Georgia[16] and New York[17] law, found an exception based on a duty to safeguard information (at least for purposes of stating a claim at the outset of a case). Typically, however, the economic loss rule bars negligence claims in cybersecurity breach cases that are based on lost profits or lost opportunity costs (despite arguments for finding a special relationship)[18] and, as previously noted, a plaintiff's

---

[16]*See In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1321-28 (N.D. Ga. 2019) (denying defendant's motion to dismiss claims for negligence and negligence *per se* under Georgia law, holding that the economic loss rule—which "generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort. In other words, 'a plaintiff may not recover in tort for purely economic damages arising from a breach of contract.' "—does not apply under Georgia law where "an independent duty exists under the law, . . ." which the court found existed because "entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information[.]") (citing other cases).

[17]*See Patton v. Experian Data Corp.,* No. SACV 15-1871 JVS (PLAx), 2016 WL 2626801, at *3 (C.D. Cal. May 6, 2016) (denying defendant's motion to dismiss New York negligence claims arising out of security breach because under the independent-duty exception under New York law, a plaintiff may recover economic damages in a tort case where (1) "a focused duty flows to a definable and manageable class comprised of individuals with a relationship so close as to approach that of privity" or (2) where the defendant "created a duty to protect the plaintiff."), *citing In re Facebook, Inc., IPO Securities & Derivative Litig*., 986 F. Supp. 2d 428, 481-82 (S.D.N.Y. 2013).

[18]*See, e.g., In re SuperValu, Inc*., 925 F.3d 955, 962-64 (8th Cir. 2019) (affirming dismissal of claims for negligence, finding no special relationship between vendor and customer and holding that plaintiff could not premise a negligence claim on an alleged violation of the Federal Trade Commission Act, which does not provide for a private right of action; "In Illinois, generally there is no affirmative duty to protect another from a criminal attack unless one of four historically recognized 'special relationships' exists between the parties. . . . The failure of Illinois law to impose this type of common-law duty on merchants mandates dismissal of Holmes's negligence claim."); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *6 (N.D. Cal. July 28, 2021) (dismissing with prejudice plaintiff's negligence claim where plaintiff was in privity of contract for the sale of goods with defendant and could not allege a special relationship); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *8-9 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's negligence claim in a data breach putative class action suit because plaintiff's claim for the value of lost time constituted an economic loss and the plaintiff could not plead the existence of a special relationship); *Bellwether Community Credit Union v. Chipotle Mexican Grill, Inc.*, 353 F. Supp. 3d 1070, 1083-85 (D. Colo. 2018) (dismissing plaintiff-credit unions' Colorado negligence claims in a security breach case as barred by the eco-

nomic loss rule because Chipotle's relationship to plaintiffs arose out of a series of contractual agreements); *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1246 (D. Colo. 2018) (dismissing plaintiff's negligence claim in a security breach case based on the economic loss rule, under either California or Colorado law, and finding no special relationship because the parties were in privity of contract because the plaintiff purchased food at defendant's restaurant); *SELCO Community Credit Union v. Noodles & Co.*, 267 F. Supp. 3d 1288, 1293-97 (D. Colo. 2017) (dismissing plaintiff-credit union's negligence and negligence *per se* claims under Colorado law as barred by the economic loss rule where (1) the duties allegedly breached by the defendant were contained in network of interrelated contracts between bank associations, issuing banks, and credit card holders, on the one hand, and bank associations, acquiring banks, and merchants such as the defendant, on the other, (2) Visa and MasterCard's rule required merchants to comply with the PCI DSS and established best practices for data security, and (3) the plaintiff had not alleged any independent duty outside these contractual provisions; "It makes no difference that Noodles & Company's contractual duties arise from a web of interrelated agreements coordinated by Visa and MasterCard rather than bilateral contracts between the merchant and plaintiffs. 'The policies underlying the application of the economic loss rule to commercial parties are unaffected by the absence of a one-to-one contract relationship. Contractual duties arise just as surely from networks of interrelated contracts as from two-party agreements.' " (citation omitted)); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc*., Case No.: 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016) (dismissing plaintiff's negligence claim as barred by the economic loss doctrine, which applies to "costs associated with time spent and loss of productivity . . . ."); *Castillo v. Seagate Technology, LLC*, Case No. 16-cv-01958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016) (dismissing plaintiffs' negligence claims arising out of a security breach based on the economic loss rule where a special relationship could not be shown); *In re Sony Gaming Networks & Customer Data Security Breach Litig.*, 903 F. Supp. 2d 942, 961 n.15 (S.D. Cal. 2012) ("Although purely economic loss usually occurs in the form of lost profits, it may also include consequential damages, loss of expected proceeds, lost opportunities, diminution in the value of the allegedly defective property, the costs of repair and replacement, loss of use, loss of goodwill, and damages paid to third parties as a result of a defendant's negligence.").

In *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019) and *Flores-Mendez v. Zoosk, Inc*., No. C 20-04929 WHA, 2021 WL 308543, at *3 (N.D. Cal. Jan. 30, 2021) a court held that lost time was not a purely economic loss under California law, but the court did so in each case without citing any California authority for what constitutes an economic loss under California law, and California law is to the contrary. *See North American Chemical Co. v. Superior Court,* 59 Cal. App. 4th 764, 777, 69 Cal. Rptr. 2d 466, 472 n. 8 (2d Dist. 1997) ("Although purely economic loss usually occurs in the form of lost profits, it may also include consequential damages, loss of expected proceeds, lost opportunities, diminution in the value of the allegedly defective property, the costs of repair and replacement, loss of use, loss of goodwill, and damages paid to third

parties as a result of a defendant's negligence."); *see also Aas v. Superior Court,* 24 Cal. 4th 627, 645 n.11, 101 Cal.Rptr.2d 718 (2000) (disagreeing with the conclusion in *North American Chemical* that the economic loss rule applied narrowly to claims against manufacturers for the negligent provision of goods, and not services, which it characterized as based on a misconception that the special relationship exception recognized in *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979) "displaces the general rule" prohibiting recovery of economic loss in negligence when a harm is foreseeable). A federal court in a case based on diversity jurisdiction must apply the law of a state's highest court. *See, e.g., Edgerly v. City & County of San Francisco,* 713 F.3d 976, 982 (9th Cir. 2013) ("In the absence of a controlling California Supreme Court decision we follow decisions of the California Court of Appeals unless there is convincing evidence that the California Supreme Court would hold otherwise.").

While the California Supreme Court has not passed on the issue of whether the risk of limitless liability is a concern in cybersecurity cases, it did explain, in the context of the economic loss rule, that:

> [P]urely economic losses "proliferate more easily than losses of other kinds" and "are not self-limiting" in the same way. (Restatement T.D. 1, § 1, com. c.) Those characteristics, the Restatement explains, threaten "liabilities that are indeterminate and out of proportion to [a defendant's] culpability," and with them "exaggerated pressure to avoid an activity altogether." (Restatement T.D. 1, § 1, com. c.) . . . . Only when the foregoing considerations are "weak or absent" — such as in *Biakanja* and *J'Aire*, but not in *Bily* — does a duty to guard against purely economic losses exist under the Restatement approach to negligence claims. (See Restatement T.D. 1, supra, § 1, com. d; see also Restatement T.D. 2, supra, § 7, com. a [using Madison's facts and the court's holding as an illustration of the Restatement view].)

Southern California Gas Leak Cases, 7 Cal. 5th 391, 407-08 & n.8, 247 Cal. Rptr. 3d 632, 645-46 & n.8 (2019).

Some district courts have allowed claims to proceed notwithstanding the economic loss rule in cases involving medical information, "the disclosure of which leads to damages that are not necessarily as 'economic' as those resulting from the theft of credit card information and social security numbers." *Stasi v. Inmediata Health Group Corp*., 501 F. Supp. 3d 898, 913-14 (S.D. Cal. Nov. 2020); *see also In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation*, __ F. Supp. 3d __, 2020 WL 2214152, at *4 (S.D.Cal. 2020) (holding that plaintiff's claim for lost time and productivity was not barred by the economic loss doctrine, in a case involving theft of medical information). These cases ultimately rely upon *Bass v Facebook,* however, which, as noted above, did not adequately consider controlling California law.

Bass, Zoosk and similar cases also may be explained in terms of the low threshold that some judges apply at the pleading stage. *See, e.g., Flores-Mendez v. Zoosk, Inc.*, No. C 20-04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021) ("The consuming public has come to believe that the internet companies, which take in their private information, have taken adequate security steps to protect the security of that information from any and all hackers or interventions. The ordinary consumer, however, has no clue what internet companies' security steps are. There would be no way for users to know what security steps were actually in

inability to plead or prove damage will be fatal to the claim.

Claims for negligence *per se*, in those jurisdictions where recognized as a separate cause of action[19] based on violation of a statutory duty, may fail where there is no statutorily recognized liability imposed on companies that experience a data breach.[20] Courts likewise have held that a negligence

---

place. Therefore, when a breach occurs, the thing speaks for itself. The breach would not have occurred but for inadequate security measures, or so it can be reasonably inferred at the pleadings stage.").

[19]Negligence *per se* is not recognized as a separate cause of action in all states. *See, e.g., Gordon v. Chipotle Mexican Grill, Inc*., No. 17-CV-1415-CMA-MLC, 2018 WL 3653173, at *19 (D. Colo. Aug. 1, 2018) (holding that California does not recognize a separate cause of action for negligence *per se*; "In [California], alleged violations of safety statutes are simply evidence of negligence." (citations omitted)), *report and recommendation adopted in relevant part,* 344 F. Supp. 3d 1231, 1246 (D. Colo. 2018); *In re Kaplan*, No. 3:11-CV-00772-RCJ, 2011 WL 6140683, at *2 (D. Nev. Dec. 9, 2011) ("Negligence *per se* is not a separate cause of action but a doctrine whereby the floor for the duty of care is set as a matter of law, taking away from the fact-finder the 'reasonable person' determination and leaving to the fact-finder only a determination of causation and damages, in cases where: (1) the plaintiff can show that the defendant has violated a duty imposed by a criminal or regulatory statute; (2) the plaintiff is a member of the class of persons intended to be protected by the statute or regulation; and (3) the harm is of the kind intended to be prevented by the statute.") (citing *Ashwood v. Clark Cty*., 930 P.2d 740, 743–44 (Nev. 1997)); *Johnson v. Enriquez*, 460 S.W.3d 669, 673 (Tex. App. 2015) ("Negligence *per se* is not a separate cause of action independent of a common-law negligence cause of action. . . . Rather, negligence *per se* is merely one method of proving a breach of duty, a requisite element of any negligence cause of action. . . . As explained by the Supreme Court, '[n]egligence *per se* is a tort concept whereby a legislatively imposed standard of conduct is adopted by the civil courts as defining the conduct of a reasonably prudent person.' ") (quoting *Carter v. William Sommerville and Son, Inc*., 584 S.W.2d 274, 278 (Tex.1979)).

[20]*See, e.g.*, *Community Bank of Trenton v. Schnuck Markets, Inc*., 887 F.3d 803, 818-19 (7th Cir. 2018) (holding, under Illinois and Missouri law, that negligence *per se* claims could not be maintained because under the laws of both states a plaintiff must show that a statute or ordinance has been violated, and while both state legislatures enacted security breach notification laws, they declined to impose liability for data breaches); *In re SuperValu, Inc., Customer Data Security Breach Litig*., 925 F.3d 955, 963-64 (8th Cir. 2019) (affirming dismissal of plaintiff's negligence claim, where Illinois law imposed no duty of care owed by the defendant to the plaintiff to protect financial information from hackers); *Cooney v. Chicago Public Schools,* 407 Ill. App. 3d 358, 943 N.E.2d 23, 27-29 (2010) (finding no duty under Illinois law to safeguard private information, in a case where Social Security numbers and other personal information of more than 1,700 former school employees were disclosed in a mailing).

per se claim may not be premised on alleged violations of the Federal Trade Act[21] (although some courts have allowed

[21]*See, e.g.*, *In re SuperValu, Inc.*, 925 F.3d 955, 963-64 (8th Cir. 2019) (affirming dismissal of plaintiff's negligence claim premised on an alleged violation of the Federal Trade Commission Act where "Congress empowered the Commission—and the Commission alone—to enforce the FTCA. Implying a cause of action would be inconsistent with Congress's anticipated enforcement scheme."); *In re Sonic Corp. Customer Data Security Breach Litigation (Financial Institutions)*, Mdl No. 2807, 2020 WL 3577341, at *6 (N.D. Ohio July 1, 2020) (dismissing plaintiffs' negligence *per se* claim premised on the FTC Act; "because the FTC Act Section 5 does not lay out objective standards, it does not support a claim for negligence per se under Oklahoma law."); *In re Brinker Data Incident Litig.*, Case No. 3:18-cv-686-J-32MCR, 2020 WL 691848, at *9 (M.D. Fla. Jan 27, 2020) (dismissing plaintiff's negligence *per se* claim in a security breach case where plaintiffs alleged that Brinker failed to comply with FTC "guidelines" and "recommendations," not any specific duty of reasonable care mandated by the FTC Act, and Florida law does not allow a negligence *per se* claim to be premised on breach of a federal statute that does not provide for a cause of action, noting, however, that plaintiffs potentially could "use the FTC Act as evidence that the data breach was within the foreseeable zone of risk."); *SELCO Community Credit Union v. Noodles & Co.*, 267 F. Supp. 3d 1288, 1293-97 (D. Colo. 2017) (holding that plaintiff-credit union's negligence and negligence *per se* claims under Colorado law were barred by the economic loss rule where (1) the duties allegedly breached by the defendant were contained in network of interrelated contracts between bank associations, issuing banks, and credit card holders, on the one hand, and bank associations, acquiring banks, and merchants such as the defendant, on the other, (2) Visa and MasterCard's rule required merchants to comply with the PCI DSS and established best practices for data security, and (3) the plaintiff had not alleged any independent duty outside these contractual provisions); *Community Bank of Trenton v. Schnuck Markets, Inc.*, 210 F. Supp. 3d 1022, 1041 (S.D. Ill. 2016) (rejecting the proposition that § 45(a) creates a duty enforceable through an Illinois negligence action in a cybersecurity breach case); *see also Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 818-19 & n.7 (7th Cir. 2018) (affirming dismissal of negligence *per se* claims under Illinois and Missouri law because the legislatures of those states chose not to create a private cause of action when they enacted security breach statutes, noting that "Plaintiffs allege a violation of the Federal Trade Commission Act, 15 U.S.C. § 45, but they do not point to any FTC interpretations or court interpretations that extend its coverage to financial institutions in merchant data breach cases.").

In *In re The Home Depot, Inc., Customer Data Security Breach Litig.*, No. 1:14-md-2583-TWT (MDL No. 2583), 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016), the court denied defendant's motion to dismiss plaintiffs' negligence *per se* claim under Georgia law, premised on an alleged FTC Act violation, but that opinion, premised on a prediction of Georgia law, has been criticized as wrongly decided. *See McConnell v. Dep't of Labor*, 337 Ga. App. 457, 787 S.E.2d 794, 797 n.4 (2016), *vacated on other grounds,* 302 Ga. 18, 805 S.E.2d 79 (2017); *Community Bank of*

claims based on alleged FTC Act violations[22]).

Trenton v. Schnuck Markets, Inc., 887 F.3d 803, 819 & n.8 (7th Cir. 2018) (criticizing *Home Depot*'s holding allowing a bank to state a negligence *per se* claim against a retail merchant as not persuasive and "based on a prediction of Georgia law that seems to have been incorrect."); *see also Department of Labor v. McConnell*, 305 Ga. 812, 828 S.E.2d 352 (2019) (affirming dismissal of plaintiff's negligence claim, in a suit where a Department of Labor employee who had inadvertently sent an email that included a spreadsheet containing the private information of individuals who had applied for unemployment benefits and other services from the Department, because there is no general legal duty to all the world not to subject others to an unreasonable risk of harm nor could one be inferred from Georgia's security breach notification statute). *But see In re Rutter's Inc. Data Security Breach Litigation*, 511 F. Supp. 3d 514, 530 n.7 (M.D. Pa. 2021) (distinguishing *Supervalu* and *Schnuck* because "[b]oth relied on Illinois law, and Illinois state courts have explicitly declined to recognize any duty to safeguard personal information."); *In re Marriott International, Inc., Customer Data Security Breach Litigation*, 440 F. Supp. 3d 447, 477-78 (D. Md. 2020) (recognizing that while Illinois law precluded the imposition of a legal duty on company for the negligence claims brought under Illinois law, the plaintiffs alleging negligence under Florida law had adequately stated a claim); *In re Equifax, Inc., Customer Data Security Breach Litigation*, 371 F. Supp. 3d 1150,1173-76 (N.D. Ga. 2019) (denying defendant's motion to dismiss Georgia negligence *per se* claims premised on alleged violations of the FTC Act and the Gramm-Leach-Bliley Act because Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence *per se* if the plaintiff can show that it is within the class of persons intended to be protected by the statute and that the statute was meant to protect against the harm suffered; "The determinative factor in *Schnuck* was that the financial institutions and retailer were in the same 'network of contracts' for payment card systems. In contrast, the Plaintiffs here do not allege that Equifax is part of this "network of contracts." Equifax is not akin to a retailer who is part of this web of a payment card system. In fact, the Schnuck court itself acknowledged this distinction,"); *see also Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760-61 (C.D. Ill. 2020) (dismissing plaintiff's negligence *per se* claim as barred by the economic loss doctrine, in putative class action brought against a supermarket chain following exposure of payment card information through a data breach caused by malware, but stating in *dicta* that "the FTC Act can serve as the basis of a negligence per se claim.").

[22]*See, e.g.*, *Purvis v. Aveanna Healthcare, LLC,* __ F. Supp. 3d __, 2021 WL 5230753, at *8-10 & n.9 (N.D. Ga. 2021) (holding that plaintiff stated a claim that defendant breached a duty to implement reasonable security measures to protect plaintiff's information, at least in a case involving sensitive protected health information); *In re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 19-md-2879, 2020 WL 6290670, at *10-13 (D. Md. Oct. 27, 2020) (holding that plaintiffs stated a claim for negligence under Maryland law based on an alleged violation of the FTC Act); *In re Marriott International, Inc., Customer Data Security Breach Litigation*, 440 F. Supp. 3d 447, 477-78 (D.

Breach of contract, breach of implied contract and unfair competition claims may fail in data breach cases where there has been no economic loss since damage (and not merely nominal damage) typically is an element of each of those claims.[23]

Md. 2020) (denying defendant's motion to dismiss plaintiffs' *per se* negligence claim under Florida law, while acknowledging that no claim could be brought based on Illinois law); *In re Equifax, Inc., Customer Data Security Breach Litig*., 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019); *In re Arby's Restaurant Group Inc*. Litig., No. 1:17-CV-0514-AT, 2018 WL 2128441, at *8-10 (N.D. Ga. Mar. 5, 2018); *First Choice Fed. Credit Union v. Wendy's Co*., No. 16-506, 2017 WL 9487086, at *3-4 (W.D. Pa. Feb. 13, 2017), *report and recommendation adopted*, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017) (following *Home Depot* and declining to dismiss negligence *per se* claim based on Section 5 of the FTC Act); *In re The Home Depot, Inc., Customer Data Security Breach Litig*., M.D.L. Docket No. 2583, 2016 WL 2897520, at *4 (N.D. Ga. May 17, 2016).

These cases relied upon *In re The Home Depot* (or cases which relied upon *Home Depot*), which, as discussed in the preceding footnote, has been criticized as wrongly decided and not a fair prediction of Georgia law.

[23]*See, e.g.*, *Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *3-6 (N.D. Cal. July 28, 2021) (dismissing with prejudice, for failure to adequately allege injury, plaintiff's breach of contract, negligence, and California unfair competition claims based on amended allegations of loss of value of PII (applying *Pruchnicki* to a claim brought under California law, where plaintiff did not allege that he had been unable to sell, profit from, or monetize his personal information and the court inferred that an expired credit card in any case had no value), risk of future harm (where plaintiff alleged he canceled the credit cards associated with the breach and that those cards had expired), out of pocket expenses and lost time (where plaintiff failed to allege that credit monitoring services were "reasonable and necessary"), and benefit of the bargain); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *9-10 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' breach of contract claim (premised on a company's Terms of Service and Privacy Policy), in a putative cybersecurity breach class action suit, because (1) nominal damages do not suffice to show legally cognizable injury under California law, (2) the alleged lost benefit of the bargain is not sufficient to allege damages because Quora's services were free and plaintiffs could not allege that the services they received were worth less as a result of the alleged breach, and (3) out-of-pocket mitigation expenses associated with the alleged data breach were not legally cognizable where plaintiffs had not suffered from identity theft—and alleged "only that they [we]re at an increased risk of identity theft—and therefore "there [we]re no damages to mitigate."); *Castillo v. Nationstar Mortg. LLC*, 15-CV-01743, 2016 WL 6873526, at *3 (N.D. Cal. Nov. 22, 2016) ("[n]ominal damages, speculative harm, or threats of future harm do not suffice to show a legally cognizable injury" for a breach of contract claim); *In re Anthem,Inc. Data Breach Litig*., No. 15-MD-02617-LHK, 2016 WL 3029783, at *12 (N.D. Cal. May 27, 2016) (holding that alleging nominal damages was insufficient to state

Courts have generally been unreceptive to breach of express or implied contract claims premised on a contract allegedly incorporating data security (or privacy) promises to prevent a breach, or arguments that the contract price contemplated the provision of data security services or notice or did not fully compensate consumers for their information (absent express terms undertaking those commitments where there was privity of contract or a provision making the consumer an intended beneficiary of a third party contract).

Contract claims arising out of a data breach may be barred by their express terms,[24] due to the absence of recoverable damage (based on theories such as "overpayment" for goods or services that implicitily included security or privacy promises[25] or the expenses of mitigating future identity theft[26]), or

---

a claim for breach of contract in a cybersecurity breach case); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009), *aff'd*, 380 F. App'x 689 (9th Cir. 2010) (affirming dismissal of a breach of contract claim in a data breach putative class action suit because nominal damages are not recoverable).

[24]*See, e.g.*, *Bray v. Gamestop Corp*., 1:17-cv-1365, 2018 WL 11226516, at *5 (D. Del. Mar. 16, 2018) (dismissing plaintiffs' express contract claim, in a putative data breach class action suit, where plaintiffs didn't plausibly plead the existence of a contract pursuant to which Gamestop agreed to certain data security measures); *In re Zappos.com, Inc*., No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) (dismissing plaintiffs' express and implied contract claims; "The only allegations alleged to give rise to any contract are that customers agreed to pay money for goods and that statements on Zappos's website indicated that its servers were protected by a secure firewall and that customers' data was safe. The first type of contract for the sale of goods is not alleged to have been breached, and the unilateral statements of fact alleged as to the safety of customers' data do not create any contractual obligations, although if negligently or intentionally false, such statements can be the basis of misrepresentation claims in tort.").

[25]*See, e.g.*, *Dinerstein v. Google, LLC,* 484 F. Supp. 3d 561, 591-92 (N.D. Ill. 2020) (dismissing plaintiff's breach of contract claim, in a putative data privacy class action suit brought against a research hospital whose electronic health records had been disclosed for research purposes to create predictive health models, for inadequately alleging money damages by claiming that he "overpaid" for services provided because of the value of his information; "He asserts that he is entitled to 'restitution on the basis that he did not receive the full benefits of his payments to the University.' . . . At most, this allegation suggests that some indeterminate amount of the price he paid for his treatments represents the cost of the University's privacy practices. This court agrees with others that have found such allegations to be insufficient."); *see also In re SAIC Corp.,* 45 F.

Supp. 3d 14, 30 (D.D.C. 2014) (ruling that plaintiff lacked standing to assert claims based on the alleged loss of value of their information caused by a security breach—which has a lower proof threshold than a claim for damages for breach of contract— in a putative data breach class action suit; "To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing. . . . Plaintiffs have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid. Nothing in the Complaint makes a plausible case that Plaintiffs were cheated out of their premiums.").

In *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 13 (D.D.C. 2019), *appeal dismissed,* 969 F.3d 412 (D.C. Cir. 2020), Judge Christopher Cooper rejected the plaintiffs' theory that they had been denied the benefit of their bargain by "broadly alleg[ing] that some indeterminate amount of their health insurance premiums went towards providing data security" and "alleg[ing] only in a conclusory fashion that the services they received were of a diminished value." He granted reconsideration, however, based on conflicting D.C. case authority suggesting that damages was not an element of a claim for breach of contract under D.C. law. *See Attias v. CareFirst, Inc.*, 518 F. Supp. 3d 43, 52 (D.D.C. 2021).

In contrast to the majority of courts elsewhere in the country, Northern District of California Judge Koh has generally embraced the benefit-of-the-bargain theory, at least for purposes of considering motions to dismiss at the outset of cybersecurity data breach cases. *See In re Yahoo! Inc. Customer Data Security Breach Litigation*, 313 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018) (concluding that plaintiff's "allegations are sufficient to allege that he suffered benefit-of-the-bargain losses" because he "pleads that he has paid $ 19.95 each year since December 2007 for Yahoo's premium email service," which was supposed to be "secure," and he would not have signed up "had he known that Yahoo's email service was not as secure as [Yahoo] represented"); *In re Anthem, Inc. Data Breach Litigation*, No. 15-md-2617, 2016 WL 3029783, at *12–15 (N.D. Cal. May 27, 2016) (holding that California plaintiffs stated a claim for breach of contract based on the "loss of benefit of the bargain" and loss of the value of their PII, while dismissing with prejudice plaintiffs' request for Benefit of the Bargain Losses under the New Jersey breach of contract claim); *In re Anthem, Inc. Data Breach Litigation*, 162 F. Supp. 3d 953, 992, 995 (N.D. Cal. 2016) (adopting "loss of benefit of the bargain" theory of "actual harm" for New York plaintiffs who alleged they had contracted for "reasonable and adequate security measures" that Anthem failed to deliver, causing plaintiffs to overpay for their health insurance).

[26] *See, e.g.*, *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *3-6 (N.D. Cal. July 28, 2021) (dismissing with prejudice, for failure to adequately allege injury, plaintiff's negligence, breach of contract, and California unfair competition claims based on amended allegations of loss of value of PII (applying *Pruchnicki* to a claim brought under California law, where plaintiff did not allege that he had been unable to sell, profit from, or monetize his personal information and the court inferred that an expired credit card in any case had no value), risk

where there was no reliance by a consumer on its provisions.[27] Express limitation of liability provisions may preclude and similar claims for breach of implied contract, and quasi contract claims (including claims for the breach of the duty

---

of future harm (where plaintiff alleged he canceled the credit cards associated with the breach and that those cards had expired), out of pocket expenses and lost time (where plaintiff failed to allege that credit monitoring services were "reasonable and necessary"), and benefit of the bargain); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *3-7 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's breach of contract claim in a data breach putative class action suit because, among other things, plaintiff could not plead a cognizable injury by alleging the future risk of identity theft, the loss of value of his PII, out of pocket expenses for credit monitoring, and the benefit of the bargain); *Attias v. CareFirst, Inc*., 518 F. Supp. 3d 43, 55 (D.D.C. 2021) (denying reconsideration of the court's prior order dismissing plaintiff's breach of contract claim, to the extent premised on the expenses of mitigating future identity theft, which the court held was not an element of recoverable breach of contract damages under D.C. law); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *9-10 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' breach of contract claim (premised on a company's Terms of Service and Privacy Policy), in a putative cybersecurity breach class action suit, because, among other things, out-of-pocket mitigation expenses associated with the alleged data breach were not legally cognizable under California law where plaintiffs had not suffered from identity theft—and alleged "only that they [we]re at an increased risk of identity theft—and therefore "there [we]re no damages to mitigate.").

In contrast to breach of contract damages, Judge Cooper, in *Attias,* granted reconsideration and reinstated claims under the consumer protection laws of Virginia and Maryland (Va. Code Ann. § 59.1-204; Md. Code Ann., Com. Law § 14-308), which require allegations of actual damages to state a claim (Va. Code Ann. § 59.1-204(a); Md. Code Ann., Com. Law § 13-408(a)), because he held, in a matter of apparent first impression, that damages under those statutes could include expenses to mitigate future identity theft. 2021 WL 311000, at *9-10.

As noted earlier in this chapter, some circuits accept mitigation expenses to support Article III standing, in some instances, depending on the facts of a given case. *See supra* § 27.07[2]. The threshold for establishing Article III standing, however, is lower than for stating a claim for breach of contract.

[27]*See, e.g.*, *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1331-32 (N.D. Ga. 2019) (granting defendant's motion to dismiss breach of contract claims premised on Equifax's Privacy Policy in a putative data breach class action suit, where the plaintiffs did "not explicitly allege[] that they read the Privacy Policy, or otherwise relied upon or were aware of the representations and assurances made in the Privacy Policy when choosing to use the Defendants' services. Without such a showing, the Plaintiffs have failed to establish the essential element of mutual assent.").

of good faith and fair dealing).[28] Contractual damage limitations further may bar a contract claim if the only damages alleged are excluded by contract.[29] Similarly, a merger clause

---

[28]*See, e.g.*, *Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *9 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's breach of express and implied contract and breach of implied covenant of good faith and fair dealing, based on the disclaimer of warranties provision in Walmart's Terms of Use, in a putative cybersecurity breach class action suit); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *10-11 (N.D. Cal. Dec. 19, 2019) (dismissing claims for breach of implied contract and breach of the covenant of good faith and fair dealing in a putative cybersecurity breach class action suit, as barred by the express disclaimer of warranties and limitation of liability provision contained in Quora's Terms of Service); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037-38 (N.D. Cal. 2019) (dismissing claims for breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, quasi contract, and breach of confidence in a putative data security breach class action suit, where Facebook's Terms of Service included a limitation-of-liability clause); *see also Adkins v. Facebook, Inc.,* No. C 18-05982 WHA, 2019 WL 3767455 (N.D. Cal. Aug. 9, 2019) (denying in relevant part plaintiff's motion to amend his Complaint, and enforcing contractual waiver provisions in a data breach case over unconscionability objections).

A breach of confidence claim, although alleged in *Bass,* rarely is asserted in cybersecurity breach cases because it requires a showing that a plaintiff conveyed confidential *and novel* information to a defendant, who then breached that confidence. *See, e.g.*, *Berkla v. Corel Corp.*, 302 F.3d 909, 917 (9th Cir. 2002). "[T]he tort of breach of confidence is grounded on an implied-in-law or quasi-contractual theory . . . . California courts have made clear that these two causes of action are mutually exclusive." *Id.* at 918; *see generally supra* § 13.03 (analyzing breach of confidence claims in connection with idea misappropriation).

[29]*See, e.g.*, *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1331-32 (N.D. Ga. 2019) (granting defendant's motion to dismiss breach of contract claims premised on Equifax's Privacy Policy, because "even if the Plaintiffs establish[ed] that the Privacy Policy was part of this express contract, the terms of the agreement provide that Equifax will not 'be liable to any party for any direct, indirect, special or other consequential damages for any use of or reliance upon the information found at this web site.' Thus, even assuming the Privacy Policy was incorporated by reference, under the terms of this agreement the Plaintiffs cannot seek damages relating to the information in Equifax's custody.").

Some statutory obligations may not be waived. For example, Alaska, Arkansas, Colorado, the District of Columbia, Hawaii, Illinois, Kentucky, Maryland, Minnesota, Nebraska, Nevada, North Carolina, Ohio, Utah, Vermont, the U.S. Virgin Islands and Washington, provide that any waiver of the requirements of their security breach notification laws is contrary to public policy and is void and unenforceable. *See generally infra* § 27.08[11]. Likewise, Massachusetts law provides that a person that experienced a breach of security "shall not require a resident to waive the

in a user agreement may preclude any claim for implied contract.[30]

A claim for breach of an implied contract may also fail if the plaintiffs can't allege that they read or even saw the purported documents constituting the contract.[31] Plaintiffs further may have difficulty establishing the existence of an implied contract if the terms of the alleged contract cannot be reasonably inferred from the surrounding circumstances (such as an implied obligation to provide data security protection or notification).[32]

---

resident's right to a private right of action as a condition of the offer of credit monitoring services." Mass. Gen. Laws Ann. ch. 93H, § 3A(b); *see generally infra* § 27.08[9].

[30]*See, e.g.*, *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1332-33 (N.D. Ga. 2019) (granting defendant's motion to dismiss breach of implied contract claim premised on Equifax's Privacy Policy; "the Equifax Terms of Use contained a valid merger clause. Such a clause precludes the assertion of an implied contract claim.").

[31]*See, e.g.*, *Krottner v. Starbucks Corp.,* 406 F. App'x 129, 131-32 (9th Cir. 2010) (affirming dismissal of plaintiffs' implied contract claims, in a suit arising out of a security breach caused when a laptop was stolen).

[32]*See, e.g.*, *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14–1152RSL, 2015 WL 4940371, at *3 (W.D. Wash. Mar. 27, 2015) (dismissing plaintiffs' implied contract claim, in a putative cybersecurity breach class action suit, because "if there were an implied contract between the parties, its terms involved only the provision of and payment for food, not a promise to safeguard the customer's credit or debit card information. . . . Plaintiff alleges no facts suggesting that he requested or that defendant made additional promises regarding loss prevention, and neither the circumstances nor common understanding give rise to an inference that the parties mutually intended to bind defendant to specific cybersecurity obligations. To the extent plaintiff expected defendant to utilize the Payment Card Industry Data Security Standard or to check its audit logs on a daily basis, such unilateral and subjective expectations do not give rise to enforceable contracts."); *In re Zappos.com, Inc*., No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) (dismissing plaintiffs' implied and express contract claims; "The only allegations alleged to give rise to any contract are that customers agreed to pay money for goods and that statements on Zappos's website indicated that its servers were protected by a secure firewall and that customers' data was safe. The first type of contract for the sale of goods is not alleged to have been breached, and the unilateral statements of fact alleged as to the safety of customers' data do not create any contractual obligations, although if negligently or intentionally false, such statements can be the basis of misrepresentation claims in tort."); *see also Brush v. Miami Beach Healthcare Group Ltd*., 238 F. Supp. 3d 1359, 1367-69 (S.D. Fla. 2017) (holding that plaintiff could not state a claim under Florida law for breach of implied contract to protect data beyond the privacy requirements already imposed by HIPAA).

Unjust enrichment claims, where cognizable as a separate cause of action and not merely a potential element of equitable relief,[33] may fail where there is an express contract.[34] Unjust enrichment claims likewise have been rejected in data breach cases where plaintiffs sought recovery of the value of their information, where there was no evidence or allegation that the money paid by the plaintiff for goods or services would have been different but for the breach or different cybersecurity practices, policies or procedures.[35]

Courts likewise consistently reject bailment claims in se-

But see Anderson v. Hannaford Brothers Co., 659 F.3d 151, 159 (1st Cir. 2011) (affirming the district court's determination that plaintiffs stated a claim for an implied contract because the district court "correctly concluded that a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would not use the credit card data for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information.").

[33]As analyzed extensively in connection with data privacy class action litigation, a number of states do not recognize standalone claims for unjust enrichment, which they consider a form of restitution. *See supra* § 26.15 (and the cases discussed in that section).

[34]*See, e.g.*, *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *8 (N.D. Cal. July 28, 2021) (dismissing with prejudice plaintiff's unjust enrichment claim because a valid contract existed between the parties); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *12 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' unjust enrichment claim, in a putative cybersecurity breach class action suit, because, under California law, unjust enrichment is an action in quasi-contract, which does not lie when an enforceable, binding agreement exists defining the rights of the parties); *Attias v. CareFirst, Inc*., 365 F. Supp. 3d 1, 25 (D.D.C. 2019) (dismissing plaintiffs' claims for unjust enrichment in a putative data breach class action suit), *appeal dismissed,* 969 F.3d 412 (D.C. Cir. 2020).

[35]96 *See, e.g.*, *In re SuperValu, Inc., Customer Data Security Breach Litigation*, 925 F.3d 955, 966 (8th Cir. 2019) (affirming dismissal of plaintiff's unjust enrichment claim under Illinois law, where "[c]ommon sense counsels against the viability of Holmes's theory of unjust enrichment. Holmes paid for groceries, the price of which would have been the same whether he paid with cash or a credit card. He did not pay a premium 'for a side order of data security and protection.' ") (quoting *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016) (applying Arizona law)); *Carlsen v. GameStop, Inc*., 833 F.3d 903, 912 (8th Cir. 2016) (affirming dismissal of plaintiff's claim for unjust enrichment under Minnesota law, where the plaintiff alleged neither a benefit conferred in exchange for protection of his PII, nor that has he shown how GameStop's retention of his subscription fee would be inequitable).

curity breach cases.[36]

As with a number of other claims arising out of a data breach, the absence of injury, harm or damage may doom consumer protection, unfair competition and related claims.[37] Where damages and other elements of a claim may be met, violations of state or federal statutes (even those that don't provide for a private cause of action may be asserted in some but not all states as unfair competition or related claims. FTC rulings,[38] for example, are potentially actionable as violations of state unfair competition laws in some but not all jurisdictions,[39] although only if the plaintiff can show

---

[36]*See, e.g.*, *In re Target Corp. Data Security Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) ("Plaintiffs allege that third parties stole the information, not that Target wrongfully retained that information."); *In re Sony Gaming Networks & Consumer Data Security Breach Litig.*, 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008); *Richardson v. DSW, Inc.*, No. 05 C 4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005) (dismissing bailment and Illinois Consumer Fraud Act claims, in a security breach case).

[37]*See, e.g.*, *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *3-6 (N.D. Cal. July 28, 2021) (dismissing with prejudice, for failure to adequately allege injury, plaintiff's negligence, breach of contract, and California unfair competition claims based on amended allegations of loss of value of PII (applying *Pruchnicki* to a claim brought under California law, where plaintiff did not allege that he had been unable to sell, profit from, or monetize his personal information and the court inferred that an expired credit card in any case had no value), risk of future harm (where plaintiff alleged he canceled the credit cards associated with the breach and that those cards had expired), out of pocket expenses and lost time (where plaintiff failed to allege that credit monitoring services were "reasonable and necessary"), and benefit of the bargain); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *3-7 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's UCL claim in a data breach putative class action suit because, among other things, plaintiff could not plead a cognizable injury by alleging the future risk of identity theft, the loss of value of his PII, out of pocket expenses for credit monitoring, and the benefit of the bargain).

[38]*See supra* § 27.06.

[39]*See, e.g.*, *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1327-28 (N.D. Ga. 2019) (denying defendant's motion to dismiss plaintiff's claim for negligence *per se* under Georgia law in a data breach case, premised on the defendant's alleged failure to maintain reasonable security pursuant to section 5 of the FTC Act).

Similarly, Cal. Bus. & Prof. §§ 17200 *et seq.* "borrows" violations from other laws by making them independently actionable as unfair competitive claims. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143–45, 131 Cal. Rptr. 2d 29 (Cal. 2003). Under section 17200,

injury.[40] Use of free service or the risk of future harm likewise will not suffice.[41] An unfair competition claim

---

"[u]nlawful acts are 'anything that can properly be called a business practice and that at the same time is forbidden by law . . . be it civil, criminal, federal, state, or municipal, statutory, regulatory, or court-made,' where court-made law is, 'for example a violation of a prior court order.' " *Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1151–52 (9th Cir. 2008) (citations omitted); *see generally supra* §§ 6.12[6], 25.04[3].

[40]*See, e.g.*, *Shaulis v. Nordstrom, Inc.*, 865 F.3d 1, 10 (1st Cir. 2017) (holding that "a plaintiff bringing an action . . . under [Mass. Gen. Laws ch. 93A, § 2, which prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce"] must allege and ultimately prove that she has, as a result [of the statutory violation], suffered a distinct injury or harm that arises from the claimed unfair and deceptive act.") (quoting *Tyler v. Michaels Stores, Inc.*, 464 Mass. 492, 503, 984 N.E.2d 737 (2013)); *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 35-36 (2d Cir. 2017), *aff'g*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *10-13 (S.D.N.Y. Aug. 17, 2016) (affirming dismissal of plaintiffs' claims under N.Y. Gen. Bus. L. § 349 for failure to allege facts showing that they had suffered an injury cognizable under that section, in a putative class action suit based on defendants' alleged use of tracking cookies, because "§ 349 injury has been recognized only where confidential, individually identifiable information—such as medical records or a Social Security number—is collected without the individual's knowledge or consent."); *In re SuperValu, Inc.*, 925 F.3d 955, 964-65 (8th Cir. 2019) (affirming dismissal of consumer-protection claims brought under the Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA), the Illinois Personal Information Protection Act (PIPA), and the Illinois Uniform Deceptive Trade Practices Act (UDTPA), because (1) "[t]he only way to pursue a claim under PIPA is by satisfying ICFA's requirements because PIPA does not create a separate cause of action"; (2) ICFA requires that a plaintiff allege "actual pecuniary loss" which plaintiff could not do by asserting that he spent time monitoring his account, incurred a single fraudulent charge to his credit card, and expended effort to replace his card; and (3) plaintiff's claim for equitable relief under the UDTPA nonetheless required him to show that he was "likely to be damaged" by SuperValu's practices in the future (815 Ill. Comp. Stat. 510/3), which he could not allege); Cal. Bus. & Prof. Code § 17200 (requiring a plaintiff to have "suffered injury in fact and has lost money or property.").

[41]*See, e.g.*, *Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *3-9 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's UCL claim in a data breach putative class action suit because, among other things, plaintiff could not plead a cognizable injury by alleging the future risk of identity theft, the loss of value of his PII, out of pocket expenses for credit monitoring, and the benefit of the bargain); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *6-7 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' UCL claims in a putative cybersecurity breach class action suit, premised on an alleged loss of the benefit of the bargain and diminished value of PII, because "that Plaintiffs did not receive the full benefit of their bargain with Quora is not a loss of money or property

premised on misrepresentation in a Privacy Policy, Terms of Use agreement or other statement or contract, similarly will fail where a plaintiff cannot allege that he or she actually read the challenged representation.[42] The absence of justifiable reliance more generally may provide grounds for dismissal, where reliance is a necessary element of the claim.[43]

Needless to say the unfair business practices law of a given state generally would only apply where a named plaintiff is

---

because Plaintiffs did not pay for Quora's services."); *In re Yahoo! Inc. Customer Data Security Breach Litig.,* 313 F. Supp. 3d 1113, 1129-30 (N.D. Cal. 2018) (dismissing the UCL claims of certain plaintiffs who obtained free services from Yahoo and alleged that, as a result of various security breaches, they were at "substantial risk for identity theft . . . ," for failure to state a claim); *see generally supra* § 26.15 (analyzing UCL claims in privacy cases).

[42]*See, e.g.*, *In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *27-28 (N.D. Cal. Aug. 30, 2017) (dismissing plaintiffs' UCL fraud claim in a cybersecurity breach case to the extent based on defendants' alleged misrepresentation that they had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you" where plaintiffs had assented to Yahoo's Terms of Use and Privacy Policy but had not alleged they read the actual statement; "plaintiffs in misrepresentation cases must allege that they actually read the challenged representations" in order to state a claim."); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1220 (N.D. Cal. 2014) (dismissing plaintiffs' misrepresentation-based UCL claims where plaintiffs did not allege that they had read any of LinkedIn's alleged misrepresentations; "To make the reliance showing, this Court has consistently held that plaintiffs in misrepresentation cases must allege that they actually read the challenged representations."); *see also, e.g.*, *In re iPhone Application Litig*., 6 F. Supp. 3d 1004, 1018 (N.D. Cal. 2013) (granting summary judgment for the defendant on the issue of standing where none of the plaintiffs presented evidence that he or she even saw, let alone read and relied upon, the alleged misrepresentations contained in Apple's Privacy Policies); *In re LinkedIn User Privacy Litig*., 932 F. Supp. 2d 1089, 1093 (N.D.Cal.2013) (dismissing plaintiffs' claim for lack of standing because "Plaintiffs do not even allege that they actually read the alleged misrepresentation—the Privacy Policy—which would be necessary to support a claim of misrepresentation. . . . Because a causal connection between a defendant's actions and plaintiff's alleged harm is required for standing, Plaintiffs have not established standing based on an alleged misrepresentation.").

[43]*See, e.g.*, *In re Rutter's Inc. Data Security Breach Litigation*, 511 F. Supp. 3d 514, 540-45 (M.D. Pa. 2021) (dismissing plaintiff's claims under the Pennsylvania Unfair Trade Practices and Consumer Protection Law where they could not allege justifiable reliance on wrongful conduct or representations).

from that state or the transaction occurred there,[44] absent choice of law principles deeming the law of a different jurisdiction to be applicable to the dispute.[45]

Under California law, an unfair competition claim may only be maintained under section 17200[46] where a plaintiff seeks equitable relief or restitution, not damages.[47] Hence, a plaintiff must prove or allege inadequacy of legal remedies to state a claim under section 17200.[48]

A claim for declaratory relief likewise will fail as unneces-

---

[44]*See, e.g.*, *Thomas v. Kimpton Hotel & Restaurant Group, LLC,* Case No. 19-cv-01860-MMC, 2020 WL 3544984, at *4-8 (N.D. Cal. June 30, 2020) (dismissing unfair competition and consumer protection claims arising under the laws of Colorado, Maryland, Pennsylvania, New York, and Texas, for those plaintiffs who were not residents of those states and/or did not undertake transactions in those states relevant to the lawsuit, in a putative data security breach class action suit).

[45]*See generally infra* chapter 55 (choice of law).

[46]Cal. Bus. & Prof. Code § 17200.

[47]*See, e.g.*, *Thomas v. Kimpton Hotel & Restaurant Group, LLC,* Case No. 19-cv-01860-MMC, 2020 WL 3544984, at *3-4 (N.D. Cal. June 30, 2020) (dismissing plaintiffs' 17200 claim in a putative cybersecurity breach class action suit where plaintiff failed to allege facts sufficient to support either a claim for injunctive relief or a claim for restitution).

[48]*See, e.g.*, *Sonner v. Premier Nutrition Corp*., 971 F.3d 834, 843-44 (9th Cir. 2020) (affirming dismissal where plaintiff failed to allege a lack of adequate legal remedy because "the traditional principles governing equitable remedies in federal courts, including the requisite inadequacy of legal remedies, apply when a party requests restitution under the UCL and CLRA in a diversity action."); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *7 (N.D. Cal. July 28, 2021) (dismissing with prejudice plaintiff's claims for equitable relief based on *Sonner*); *Shay v. Apple Inc.*, Case No.: 20cv1629-GPC(BLM), 2021 WL 1733385 (S.D. Cal. May 3, 2021) (dismissing plaintiff's UCL claim based on *Sonner*); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *7-8 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's UCL claim in a putative data breach class action suit because, among other things, plaintiff alleged he suffered compensable damages, and rejecting the argument that plaintiff would have no adequate remedy at law if the court were to find his legal claims deficient); *In re California Gasoline Spot Market Antitrust Litigation*, Case No. 20-cv-03131-JSC, 2021 WL 1176645, at *7-8 (N.D. Cal. Mar. 29, 2021) (dismissing plaintiff's UCL claim with leave to amend if plaintiffs had a good faith basis to allege inadequacy of legal remedy); *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 662 (N.D. Cal. 2020) (granting summary judgment for the defendant on plaintiff's UCL claim in a putative data breach class action suit where plaintiff failed "to allege or demonstrate that any remedy at law is inadequate, and in fact she even seeks a remedy at law through her negligence claim, which is based on the same alleged conduct as her equitable claim.").

sary if an adequate remedy exists under some other cause of action.[49]

Breach of fiduciary duty claims generally fail in the absence of a fiduciary obligation.[50] Courts thus far have also been unwilling to impose strict liability for a data breach.[51]

---

[49]*See, e.g.*, *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *12-13 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' claims for declaratory relief in a putative cybersecurity breach class action suit as duplicative of plaintiffs' breach of contract claim, which the court also dismissed on other grounds).

[50]*See, e.g.*, *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14–1152RSL, 2015 WL 4940371, at *4 (W.D. Wash. Mar. 27, 2015) (dismissing plaintiffs' breach of fiduciary duty claim, in a putative cybersecurity breach class action suit; "Plaintiff alleges that defendant had superior knowledge of its cybersecurity practices and that plaintiff was induced to share his confidential financial information in reliance on that superior knowledge. While this argument uses all of the right words, the facts of this case are not similar to those in which a fiduciary relationship was found to exist under Washington law."). As the court explained in *Lovell*: "A fiduciary relationship can arise as a matter of law when the nature of the relationship (*i.e.*, trustee and beneficiary, principal and agent, physician and patient, husband and wife) is such that the fiduciary has a duty, compelled by his undertaking, to act primarily for the benefit of another in all matters related to the undertaking. . . . The relationship between restauranteur and patron is not of a fiduciary nature." *Id.*,*citing Van Noy v. State Farm Mut. Automobile Insurance Co*., 142 Wash. 2d 784, 797–98, 16 P.3d 574 (2001).

[51]*See, e.g.*, *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14–1152RSL, 2015 WL 4940371, at *5 (W.D. Wash. Mar. 27, 2015) (dismissing plaintiffs' strict liability claim, in a putative cybersecurity breach class action suit). As explained by Judge Lasnik in *Lovell*:

> In the civil context, there are two types of activities that trigger strict liability in Washington. The first involves "an abnormally dangerous activity" that causes harm: the actor will be liable for injuries resulting from the activity even if he has exercised the utmost care in the performance. *Klein v. Pyrodyne Corp*., 117 Wn. 2d 1, 6 (1991); Restatement (Second) of Torts § 519(1). The Court considers six factors when determining whether an admittedly dangerous activity is "abnormally dangerous," with the goal of determining whether the dangers and inappropriateness of the activity in the given locality "are so great that, despite any usefulness it may have for the community, [the actor] should be required as a matter of law to pay for any harm it causes, without the need of a finding of negligence." *Hurley v. Port Blakely Tree Farms L.P*., 182 Wash. App. 753, 332 P.3d 469, 474–77 (2014) (quoting Restatement (Second) of Torts § 520, cmt. f). Plaintiff does not argue that accepting credit cards or storing financial information is an abnormally dangerous activity. The first type of strict liability does not, therefore, apply.
>
> The manufacture, distribution, or sale of unreasonably dangerous products may also give rise to strict liability under the rule embodied in Restatement (Second) of Torts § 402A. *See Lunsford v. Saberhagen Holdings, Inc*., 166 Wash. 2d 264, 284, 208 P.3d 1092 (2009). The theory underlying this type of strict liability is that the manufacturer, seller, and/or distributor "is in the best posi-

California invasion of privacy claims arising out of security breaches have failed because the mere fact that data has been exposed, even as a result of a criminal attack, may not rise to the level of a "substantial" invasion of privacy, which is required to state a claim.[52] An Illinois invasion of privacy claim likewise was dismissed in a data breach case where the plaintiff could not allege that the breach resulted in an intrusion into private life that was intentional or a disclosure to the public at large.[53]

Claims based on delay in providing notification may fail in the absence of any actual injury proximately caused by the alleged delay.[54]

---

tion to know of the dangerous aspects of the product and to translate that knowledge into a cost of production against which liability insurance can be obtained." *Simonetta v. Viad Corp*., 165 Wash. 2d 341, 354, 197 P.3d 127 (2008). The Court has not found, and plaintiff has not identified, any case in which § 402A liability has been imposed outside the product liability context. The Court declines plaintiff's invitation to do so here.

[52]*See, e.g.*, *Schmitt v. SN Servicing Corp.*, Case No. 21-cv-03355-WHO, 2021 WL 3493754, at *7 (N.D. Cal. Aug. 9, 2021) (dismissing plaintiff's California invasion of privacy claim, distinguishing cases involving medical information); *Razuki v. Caliber Home Loans, Inc*., No. 17CV1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. Jun. 8, 2018) (dismissing plaintiff's claim for invasion of privacy under the California Constitution for failing to state a claim, in a security breach case based on the alleged disclosure of personal information because "[l]osing personal data through insufficient security doesn't rise to the level of an egregious breach of social norms underlying the protection of sensitive data like social security numbers . . . . [plaintiff's] allegations don't suggest the type of intentional, egregious privacy invasion contemplated in *Hill*."); *see generally supra* §§ 12.02, 26.07[2], 26.15 (analyzing invasion of privacy claims, respectively, in general, in privacy cases, and in connection with data privacy class action litigation).

[53]*See Sweet v. BJC Health System*, Case No. 3:20-CV-00947-NJR, 2021 WL 2661569, at *8 (S.D. Ill. June 29, 2021). As explained by the court: "Under Illinois law, a party alleging intrusion into private life must show that the intrusion was intentional. *Lovgren v. Citizens First Nat. Bank of Princeton*, 126 Ill. 2d 411, 128 Ill. Dec. 542, 534 N.E.2d 987, 988 (Ill. 1989). Public disclosure, on the other hand, requires a showing that the information was disclosed to the public at large. *Cordts v. Chicago Tribune Co*., 369 Ill. App.3d 601, 307 Ill. Dec. 790, 860 N.E.2d 444, 450 (Ill. App. 2006)." 2021 WL 2661569, at *8.

[54]*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

Claims based on negligence or a failure to warn consumers also potentially may be preempted by the Cybersecurity Information Sharing Act (CISA),[55] 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.[56] 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.[57] 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."[58]

State law may provide a safe harbor or defense for businesses that have adopted and implemented written information security programs, as addressed in greater detail in section 27.04[6]. 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 security controls resulted in a data breach.[59] 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

---

breach notification increased plaintiffs' risk of injury).

[55]6 U.S.C.A. §§ 1501 to 1510; *see generally supra* § 27.04[1.5] (analyzing the statute).

[56]6 U.S.C.A. § 1505(a); *supra* § 27.04[1.5].

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

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

[59]*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

reasonable information security controls resulted in a data breach concerning personal information[,]" where a *covered entity*[60] has created, maintains, and complies with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information[61] (or the protection of both personal information

---

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).

[60]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).

[61]*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;
  (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;

and restricted information[62]) and that reasonably conforms to an "industry recognized cybersecurity framework."[63] It further provides that a covered entity's failure or decision not to comply may not support a private cause of action.[64] The technical requirements for meeting the safe harbor are set forth in greater detail in section 27.04[6][H].[65]

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 Equifax, Inc., Customer Data Security Breach Litigation*,[66] the court denied Equifax's motion to dismiss claims brought

---

(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).

[62]*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).

[63]Ohio Rev. Code Ann. § 1354.02(D).

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

[65]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.

[66]*In re Equifax, Inc., Customer Data Security Breach Litigation*, 362

under multiple state security breach notification laws, alleging that Equifax breached statutory requirements for notice "in the most expedient time possible" and similar language in other state statutes by waiting 41 days before sending notice.

By contrast, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[67] 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 have been 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."[68] 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, or reckless conduct on behalf of Sony."[69]

In *Sony,* among other rulings, the court also dismissed

F. Supp. 3d 1295, 1342-43 (N.D. Ga. 2019)

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

[68]*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).

[69]*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

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.[70]

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 Hampshire law and allowed claims for injunctive relief under California's security breach notification law, Cal. Civil Code § 1798.84(e) (but not damages under section 1798.84(b)) and partial performance and breach of the implied duty of good faith and fair dealing,[71] even as the court dismissed multiple other claims for negligence, negligent misrepresentation/

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).

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

[71]*In re Sony Gaming Networks & Customer Data Security Breach*

omission, unjust enrichment and state consumer protection laws.

Claims also potentially may be raised in some cybersecurity breaches under the California Consumer Privacy Act (CCPA).[72] The CCPA authorizes 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[73] 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 . . . ."[74] CCPA litigation is analyzed in section 26.13A[14].

Litigation, 996 F. Supp. 2d 942, 985–92 (S.D. Cal. 2014)

[72]Cal. Civ. Code §§ 1798.100 to 1798.199; *see generally supra* § 26.13A.

[73]Cal. Civ. Code § 1798.150(a)(1).

[74]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.
  (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
  (vii) Genetic data.

(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).

As set forth in section 26.13A[14], a plaintiff may be unable to assert a claim under the CCPA[75] (or, after January 1, 2023, under the California Privacy Rights Act (CPRA))[76] in state or federal court (and potentially seek class certification) unless the plaintiff can allege that (1) the plaintiff is a resident of California, (2) the defendant is a *business* (as defined in the statute) subject to the CCPA,[77] (3) the incident occurred on or after January 1, 2020[78] and (4) resulted in the unauthorized[79] access and exfiltration, theft, or disclosure of specific *personal information* (defined more narrowly than

---

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).

Genetic data means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom. *Id.* § 1798.81.5(d)(5).

[75]Cal. Civ. Code § 1798.150(a)(1).

[76]Cal. Civ. Code § 1798.150(a)(1) (effective Jan. 1, 2023).

[77]*See, e.g.*, *In re Blackbaud, Inc., Customer Data Breach Litig.*, Case No. 3:20-mn-02972-JMC, 2021 WL 3568394, at *4-6 (D.S.C. Aug. 12, 2021) (denying defendant's motion to dismiss where the plaintiffs adequately alleged that Blackbaud was a *business* under the CCPA in a case arising out of a ransomware attack).

[78]*See, e.g.*, *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for failing to allege that the breach occurred after January 1, 2020, when the CCPA took effect, and failing to adequately allege the disclosure of personal information as defined by the statute); *see also Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *2 (N.D. Cal. July 28, 2021) (dismissing plaintiff's CCPA claim with prejudice).

[79]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized);

under the CCPA generally),[80] (5) the personal information was unencrypted or unredacted at the time when exfiltrated, stolen, or disclosed,[81] (6) the exfiltration, theft, or disclosure resulted from a business's failure to implement reasonable security measures, and (7) the plaintiff is not subject to a binding and enforceable arbitration agreement.[82] To recover statutory damages, a plaintiff must further show that it provided notice and an opportunity to cure, and that the business did not do so (as discussed later in this section).[83]

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, destruction, use, modification or disclosure—establish a duty that cannot be disclaimed and potentially invites litigation in the absence of any express definition of, or safe harbor for, what might be deemed *reasonable*. As analyzed in section 27.04[6][C], multiple other

---

[80]*See* 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 (otherwise applicable to other provisions of the CCPA) in section 1798.140(o). Thus, not all breaches will be actionable under the CCPA. *See, e.g., Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for, among other things, failing to adequately allege the disclosure of personal information as defined by the statute).

Under the CPRA, the definition of *personal information* applicable to lawsuits brought pursuant to section 1798.150(a)(1) will be expanded to also include an "email address in combination with a password or security question and answer that would permit access to the account . . . ." *Id.* § 1798.150(a)(1) (effective Jan. 1, 2023); *see generally supra* § 26.13A[14].

[81]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized);

[82]*See generally supra* § 22.05[2][M] (analyzing the enforceability of consumer arbitration claims, which under the Federal Arbitration Act and Supremacy Clause of the U.S. Constitution, will preempt inconsistent state laws or judge made rules favoring litigation of disputes). The CCPA does not purport to bar arbitration and, if it did, it would conflict with, and be preempted by, the Federal Arbitration Act. *See supra* § 22.05[2][M]. The CPRA, however, potentially seeks to restrict arbitration of claims for public injunctive relief.

[83]*See* Cal. Civ. Code § 1798.150(a)(1); *see generally supra* § 26.13A[14].

states (including Alabama, Arkansas, Colorado, Delaware, Illinois, Indiana, Kansas, Louisiana, Maryland, Nebraska, Nevada, New Mexico, Oregon, Rhode Island, South Carolina (for insurance licensees), Texas, and Utah) have enacted similar laws. Nevertheless, causation and the absence of damages may prevent a plaintiff from prevailing on such a claim. In addition, litigants have sometimes discovered that, as the FTC has acknowledged, "security breaches sometimes can happen when a company has taken every reasonable precaution."[84]

Absent a state statute that affords statutory damages or attorneys' fees, a plaintiff will be more likely to be able to state a claim where liability and causation can be established and where a security breach has led to identity theft, unauthorized charges or other financial harm.[85] For example, in

---

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

[85]*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)

Anderson v. Hannaford Brothers Co.,[86] 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."[87] The court explained that:

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

---

when two laptops containing unencrypted data were stolen from the 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*, 196 A.3d 1036 (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).

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

[87] *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.[88]

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.[89] 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."[90] 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."[91] The court noted that the fact that many banks and credit card issuers immediately

---

2011).

[88] *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).

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

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

[91] *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.[92]

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.[93]

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.[94] 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).

[92]*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.

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

[94]*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.[95]

On remand, the lower court denied plaintiffs' motion for class certification, finding that common questions of law and fact did not predominate.[96]

In *Dittman v. UPMC*,[97] 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 *Hannaford Brothers* and *Dittman*, in *Irwin v. Jimmy John's Franchise LLC*,[98] 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 *Department of Labor v. Mc-*

2011).

[95]*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).

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

[97]*Dittman v. UPMC*, 196 A.3d 1036 (Pa. 2018).

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

Connell,[99] the Georgia Supreme Court 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, among other things, 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 because the information disclosed did not affect reputation and the matters disclosed were not offensive and objectionable.[100]

In *Resnick v. AvMed, Inc.,*[101] 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

---

[99]*Department of Labor v. McConnell*, 305 Ga. 812, 828 S.E.2d 352 (2019).

[100]*See Department of Labor v. McConnell*, 305 Ga. 812, 817-19, 828 S.E.2d 352, 359-60 (2019).

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

U.S. postal service to delay plaintiff learning of the unauthorized accounts and charges. Fourteen months after the theft 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."[102]

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.[103] 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.[104]

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*,[105] 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-

---

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

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

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

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

nesses and their financial institutions.[106] *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[107] (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 . . . ."[108]

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

---

[106]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).

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

[108]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.[109]

By contrast, in *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*,[110] 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.

---

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

[110] *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."[111] For example, in *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*,[112] 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 verifi-

---

[111] *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); *see also, e.g.*, *Glen Holly Entertainment, Inc. v. Tektronix Inc.*, 343 F.3d 1000, 1015 (9th Cir. 2003) ("[G]eneralized, vague and unspecific assertions, constitut[e] mere 'puffery' upon which a reasonable consumer could not rely."); *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).

[112] *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).

able statements, rather than mere puffery, made prior to, rather than after the security breach, to the extent relied 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.[113] 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."[114]

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.[115]

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:

---

[113]*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).

[114]*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).

[115]*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).

- "We maintain current updates of network and operating system security releases and virus definitions, and 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."[116]

Similarly, in *In re Yahoo! Inc. Customer Data Security Breach Litigation*,[117] the statement that "protecting our systems and our users' information is paramount to ensur-

---

[116]*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); *see also, e.g.*, *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."). In *Heartland*, 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."

834 F. Supp. 2d at 593.

[117]*In re Yahoo! Inc. Customer Data Security Breach Litigation*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *26 (N.D. Cal. Aug. 30, 2017). By contrast, the court found potentially actionable the statement that the company had employed "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you." *Id.* The court explained that a "reasonable consumer could rely on this statement as representing that Defendants did, in fact, use safeguards that complied with federal regulations." *Id.* Likewise, "[m]ore generally, a reasonable consumer could reply on this statement as representing that Defendant's safeguards, which were represented to comply with federal

ing Yahoo users enjoy a secure user experience and maintaining our users' trust" was found to be non-actionable puffery under California's unfair competition statute because the statement was vague and an "all-but-meaningless superlative[,]"and said "nothing about the specific characteristics" of the products or services offered by the defendant, and thus could not have been relied upon by a reasonable consumer.

Fraud claims must meet heightened pleading requirements in federal court and must show knowledge of falsity at the time a statement is made.[118]

Negligent misrepresentation claims may not be viable in a data breach case when based on an alleged omission.[119]

Claims based on theft or hacking may be difficult to establish against third party businesses that are themselves victims.[120]

---

regulations, were sufficient to protect users' information from ordinary data security threats." *Id.*

[118]*See, e.g.*, *Thomas v. Kimpton Hotel & Restaurant Group, LLC,* Case No. 19-cv-01860-MMC, 2020 WL 3544984, at *7-8 (N.D. Cal. June 30, 2020) (dismissing plaintiff Martin's claim under Texas law for false statements, in a putative data breach class action suit, because Texas law requires a plaintiff to allege that the defendant knew that a representation was false or made it recklessly as a positive assertion without any knowledge of its truth, and plaintiff asserted that "Kimpton was aware that its agent, Sabre, did not have the best security standards" but failed to allege facts to support that conclusion "e.g., that Kimpton knew, at the time it made the challenged statements, Sabre used single factor authentication and that it knew such a system was insufficient to protect PII.").

[119]*See, e.g.*, *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14–1152RSL, 2015 WL 4940371, at *5-6 (W.D. Wash. Mar. 27, 2015) (dismissing plaintiffs' negligent misrepresentation claim, in a putative cybersecurity breach class action suit, because "[a]n omission is actionable only if there were a duty to disclose: in such instances, 'the suppression of a material fact is tantamount to an affirmative misrepresentation.' . . . Plaintiff has not alleged facts giving rise to a plausible inference that the disclosure of data regarding compliance with certain cybersecurity standards would be material to his decision about whether to shop or dine with a particular retailer.").

[120]*See, e.g.*, *Nowak v. Xapo, Inc.*, Case No. 5:20-cv-03643-BLF, 2020 WL 6822888, at *3-5 (N.D. Cal. Nov. 20, 2020) (dismissing plaintiff's Computer Fraud and Abuse Act claim, with leave to amend, where the plaintiff alleged that third parties hacked into his cryptocurrency exchange account, stealing 500 Bitcoins which they deposited into wallet addresses owned by custodial cryptocurrency firms Indodax and Xapo, which plaintiff alleged employed inadequate policies and procedures to prevent use of

In addition to putative class action suits, data 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.[121]

27.07[4] MDL Consolidation in Putative Data Breach class Action Litigation

Where more than one data breach suit has been filed arising out of the same incident in different federal courts, any plaintiff or defendant (or both) may seek consolidation for pre-trial purposes before the Multidistrict Litigation Panel (MDL).[1] MDL consolidation may be ordered where there are civil actions pending in more than one district that have one or more common questions of fact, and where transfer, and consolidation for pre-trial purposes in a single venue, would be for the convenience of the parties and witnesses and promote the just and efficient conduct of the cases.[2] A number of larger cybersecurity data breaches have resulted in MDL consolidation orders, while consolidation has been denied in other cases.

---

their services for malicious activity, because, among other things, the CFAA was designed to target hacking, not misappropriation, and therefore plaintiff would have to allege that a defendant engaged in hacking, and didn't merely benefit from it; dismissing plaintiffs' Cal. Penal Code § 502 claim where it was not clear that the nature of plaintiff's loss was cognizable under the statute; and dismissing plaintiffs' claim under Cal. Penal Code § 496 because plaintiff couldn't allege that Xapo knew the Bitcoins had been stolen).

[121] *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.").

[Section 27.07[4]]

[1] *See* 28 U.S.C.A. § 1407.

[2] *See* 28 U.S.C.A. § 1407(a).

There is no magic number of cases that would justify MDL consolidation, but centralization " 'should be the last solution after considered review of other options.' . . . Among these options are voluntary cooperation and coordination among the parties and the involved courts to avoid duplicative discovery or inconsistent pretrial rulings."[3] Hence, consolidation has been denied in a number of data security breach cases.[4]

When data breach cases have been consolidated, the MDL Panel typically chooses to consolidate cases in the district where the defendant's business is headquartered, as "relevant documents and witnesses thus likely will be found there."[5]

MDL consolidation under section 1407 " 'should be the last

---

[3] *In re Dickey's Barbecue Restaurants, Inc., Customer Data Security Breach Litigation,* 521 F. Supp. 3d 1355, 1356 (J.P.M.D.L. 2021) (denying consolidation), *quoting In re Best Buy Co., Inc., Cal. Song-Beverly Credit Card Act Litig*., 804 F. Supp. 2d 1376, 1378 (J.P.M.L. 2011).

[4] *See, e.g.*, *In re Dickey's Barbecue Restaurants, Inc., Customer Data Security Breach Litigation,* 521 F. Supp. 3d 1355 (J.P.M.D.L. 2021) (denying consolidation of three suits pending in the Northern District of Texas, two in the Southern District of California and one in the Central District of California); *In re StockX Customer Data Security Breach Litig.*, 412 F. Supp. 3d 1363, 1365 (J.P.M.L. 2019) (denying transfer of three data breach actions in three districts, concluding that "cooperation among the few involved courts and counsel is a workable alternative to centralization"); *In re First Am. Fin. Corp. Customer Data Security Breach Litig.*, 396 F. Supp. 3d 1372, 1373 (J.P.M.L. 2019) (denying centralization of seven data breach actions in two districts); *In re [24]7.AI, Inc. Customer Data Sec. Breach Litig.*, 338 F. Supp. 3d 1345, 1347 (J.P.M.L. 2018) (denying transfer of three data breach actions in three districts, recognizing that "a number of pending motions could significantly reduce or even eliminate the multidistrict character of this litigation"); *In re Hudson's Bay Co. Customer Data Sec. Breach Litig.*, 326 F. Supp. 3d 1372, 1373 (J.P.M.L. 2018) (denying transfer of four data breach actions in two districts).

[5] *See, e.g.*, *In re: Capital One Customer Data Security Breach Litigation*, 396 F. Supp. 3d 1364 (M.D.L. 2019) (centralizing cases in the Eastern District of Virginia); *In re Marriott Int'l, Inc.*, 363 F. Supp. 3d 1372, 1374–75 (J.P.M.L. 2019) (centralizing securities fraud putative class action suits arising out of a data breach in the district of Maryland); *In re Equifax, Inc., Customer Data Security Breach Litig.*, 289 F. Supp. 3d 1322, 1326 (J.P.M.L 2017) (centralizing actions in the Northern District of Georgia over objections about a circuit split on the issue of Article III standing); *In re Home Depot, Inc.*, 65 F. Supp. 3d 1398, 1400 (J.P.M.L. 2014) (centralizing actions in the Northern District of Georgia); *In re Target Corp. Customer Data Security Breach Litig*., 11 F. Supp. 3d 1338, 1339 (MDL 2014) (transferring cases to the District of Minnesota for coordinated or consolidated pretrial proceedings more than 33 separate actions pend-

solution after considered review of all other options . . . [such as] voluntary cooperation and coordination among the parties and the involved courts to avoid duplicative discovery or inconsistent pretrial rulings.' "[6]

Even where MDL consolidation is not sought or obtained, parties may be able to coordinate cases for pretrial purposes through traditional joinder mechanisms (which in some cases may be preferable).

When cases have been consolidated, plaintiff's counsel may seek appointment of an interim lead counsel pursuant to Federal Rule of Civil Procedure 23(g) (even before the court entertains a motion for class certification) if there is rivalry or uncertainty among and between plaintiffs' counsel.[7] Designation of interim lead counsel, however, may not be necessary or appropriate absent special circumstances.[8]

---

ing in 18 districts and potential tag-along actions arising out of Target's 2013 security breach); *In re Supervalu*, 67 F. Supp. 3d 1377, 1378 (J.P.M.L. 2014) (centralizing pretrial proceedings in the District of Minnesota, where Supervalu's corporate headquarters were located, despite Supervalu's request to centralize proceedings in the District of Idaho); *In re Schnuck's Market's, Inc. Customer Data Security Breach Litig.*, 978 F. Supp. 2d 1379, 1381–82 (J.P.M.L. 2013) (centralizing actions alleging that Schnuck's data security breach compromised the financial and personal data of its customers, in the Eastern District of Missouri); *In re Zappos.com*, 867 F. Supp. 2d 1357, 1358 (J.P.M.L. 2012) (granting Zappos's motion to centralize actions in the District of Nevada); *see also In re American Medical Collection Agency, Inc., Customer Data Security Breach Litigation,* 410 F. Supp. 3d 1350, 1354 (J.P.M.L. 2019) (centralizing the litigation in the district of New Jersey where two of the defendants were headquartered and close to where a third defendant (whose headquarters was in Elmsford, New York) was located).

[6] *In re Dickey's Barbecue Restaurants, Inc., Customer Data Security Breach Litigation,* 521 F. Supp. 3d 1355, 1356 (J.P.M.D.L. 2021), *quoting In re Best Buy Co., Inc., Cal. Song-Beverly Credit Card Act Litigation*, 804 F. Supp. 2d 1376, 1378 (J.P.M.L. 2011).

[7] "In some cases . . . there may be rivalry or uncertainty that makes formal designation of interim counsel appropriate." Fed. R. Civ. P. 23 advisory committee's note (discussing former subdivision (g)(2)(A), now renumbered to (g)(3)).

[8] *See, e.g.*, *In re Google Assistant Privacy Litigation*, Case No. 19-cv-04286-BLF, 2020 WL 7342713, at *1-2 (N.D. Cal. Dec. 14, 2020) (denying motion for appointment of interim lead counsel); *In re Nest Labs Litig*., No. 14-cv-01363-BLF, 2014 WL 12878556, at *1 (N.D. Cal. Aug. 18, 2014) (denying appointment); *Donaldson v. Pharmacia Pension Plan*, No. CIV. 06-3-GPM, 2006 WL 1308582, at *1-2 (S.D. Ill. May 10, 2006) (noting that typical situation requiring appointment of interim class counsel is one

27.07[5] Preservation of Privilege and Confidentiality in Data Breach Litigation

Preserving privilege, and protecting the confidentiality of information that itself could create additional security risks to a company by exposing details of its network configuration to hackers, are potentially important issues that may arise at various stages in cybersecurity litigation.

Privilege issues may arise because, "[g]iven our increasingly complex regulatory landscape, attorneys often wear dual hats, serving as both a lawyer and a trusted business advisor."[1] Challenges to assertions of work product in security breach cases in connection with forensic reports, in particular, increased significantly following a widely publicized decision in June 2020 in *In re Capital One Consumer Data Security Breach Litigation*,[2] holding that a security incident forensic report conducted for Capital One by FireEye (doing business as Mandiant) was not entitled to work product protection[3] and therefore subject to production in a putative class action suit brought over the security incident. The decision raised concerns because companies frequently—although not always—commission forensic reports to determine the extent and severity of a security incident, and those reports potentially could overstate or misstate the extent of a breach (especially when generated quickly, shortly after a breach is uncovered or under time pressure to meet reporting or notification deadlines, before all the facts are known). For certain regulated businesses, and certain types of breaches, obtaining a forensic report may be required. In all cases, *Capital One* emboldened plaintiffs lawyers to challenge privilege more aggressively in cybersecurity breach litigation.

In *Capital One,* Judge Anthony J. Trenga, affirming and expanding on the report and recommendation of Magistrate

---

"where a large number of putative class actions have been consolidated or otherwise are pending in a single court").

[Section 27.07[5]]

[1] *In re Grand Jury*, 13 F.4th 710, 712 (9th Cir. 2021).

[2] *In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 3470261 (E.D. Va. June 25, 2020).

[3] A party may not ordinarily discover documents "that are prepared in anticipation of litigation by or for another party or its representative." Fed. R. Civ. P. 26(b)(3)(A).

Judge John F. Anderson,[4] overruled 72 objections raised by Capital One and ordered Capital One to "provide forthwith" a copy of the Mandiant report to plaintiffs' counsel. The court, applying the Fourth Circuit's "driving force" test for evaluating the propriety of work product assertions, concluded that the driving force behind preparation of the document was business a business purpose, not litigation.

The "driving force" test is not applied everywhere, however. For example, the Ninth Circuit rejects any weighing of motives when a document has a dual-purpose and will uphold work product protection for a forensic report (or other documents or information sought in discovery) even if the report was generated to serve business or security objectives, in addition to having been prepared in anticipation of litigation[5] (even as it applies "the primary-purpose test" in evaluating attorney-client communications[6]). Nevertheless, companies seeking to preserve privilege in anticipation of litigation

---

[4] *In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 2731238 (E.D. Va. May 26, 2020).

[5] *See In re Grand Jury Subpoena (Mark Torf/Torf Environmental Management)*, 357 F.3d 900, 908 (9th Cir. 2004). The Ninth Circuit has held that documents must have two characteristics to be protected under the work product doctrine: "(1) they must be prepared in anticipation of litigation or for trial, and (2) they must be prepared by or for another party or by or for that other party's representative." *Id.* at 907 (internal quotations omitted). A "because-of" test is used to determine whether a document was prepared in anticipation of litigation, which means that a document doesn't need to be prepared *exclusively* for use in litigation. *In re Experian Data Breach Litigation*, SACV 15-01592 AG (DFMx), 2017 WL 4325583, at *1 (C.D. Cal. May 18, 2017) (upholding Experian's assertion of work product protection in connection with a security incident report prepared by Mandiant), *citing Grand Jury Subpoena,* 357 F.3d at 907–08. "The 'because of' standard does not consider whether litigation was a primary or secondary motive behind the creation of a document." *Grand Jury,* 357 F.3d at 908. "Rather, it considers the totality of the circumstances and affords protection when it can fairly be said that the document was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation." *Id.* (internal quotations omitted).

[6] *See In re Grand Jury*, 13 F.4th 710, 714-17 (9th Cir. 2021). In so ruling, the Ninth Circuit contrasted its approach to work product determinations involving what it characterized as "the dual-purpose nature" of representation, explaining that:

> In the work-product context, the concern is "to preserve a zone of privacy in which a lawyer can prepare and develop legal theories and strategy with an eye toward litigation, free from unnecessary intrusion by his adversaries." *United States v. Adlman*, 134 F.3d 1194, 1196 (2d Cir. 1998) (cleaned up). In short, the work-product doctrine upholds the fairness of the adversarial process

need to account for the least protective test that may be applied in a jurisdiction where they potentially could be subject to suit (or where a third party vendor could be subpoenaed).

The *Capital One* opinion offers suggestions about how companies may preserve work product protection in connection with a forensic report commissioned following a security

---

by allowing litigators to creatively develop legal theories and strategies—without their adversaries invoking the discovery process to pry into the litigators' minds and free-ride off them. *See, e.g.*, *Allen v. Chi. Transit Auth.,* 198 F.R.D. 495, 500 (N.D. Ill. 2001) (explaining that the intent of the work-product doctrine "is to protect the adversarial process by providing an environment of privacy" and insure "that the litigator's opponent is unable to ride on the litigator's wits"). Given this goal, it makes sense to have a broader "because of" test that shields lawyers' litigation strategies from their adversaries.

In contrast, the attorney-client privilege encourages "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). Unlike the work-product doctrine, the privilege is not necessarily tied to any adversarial process, and it is not so much concerned with the fairness of litigation as it is with providing a sanctuary for candid communication about any legal matter, not just impending litigation. Applying a broader "because of" test to attorney-client privilege might harm our adversarial system if parties try to withhold key documents as privileged by claiming that they were created "because of" litigation concerns. Indeed, it would create perverse incentives for companies to add layers of lawyers to every business decision in hopes of insulating themselves from scrutiny in any future litigation. Because of these different aims, it makes sense to apply different tests for the attorney-client privilege and the work-product doctrine. *See Sanmina*, 968 F.3d at 1120 ("[W]ork-product protection is not as easily waived as the attorney-client privilege based on the distinct purposes of the two privileges." (cleaned up)).

13 F.4th at 715-16. *Compare In re Kellogg Brown & Root, Inc.,* 756 F.3d 754, 759 (D.C. Cir. 2014) (applying "a primary purpose" test rather than a test focused on finding *the* primary purpose, for assessing whether a dual purpose communication is protected by the attorney-client privilege because "trying to find the one primary purpose for a communication motivated by two sometimes overlapping purposes (one legal and one business, for example) can be an inherently impossible task . . . .").

For purposes of the work-product doctrine, the Ninth Circuit reiterated in *In re Grand Jury* in 2021 its analysis from the similarly-named *In re Grand Jury Subpoena* case from 2004, writing that:

[T]he "because of" test—which typically applies in the work-product context—"does not consider whether litigation was a primary or secondary motive behind the creation of a document." *In re Grand Jury Subpoena (Mark Torf/Torf Env't Mgmt.),* 357 F.3d 900, 908 (9th Cir. 2004). It instead "considers the totality of the circumstances and affords protection when it can fairly be said that the document was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation." *Id*. (cleaned up). It is a broader test than the "primary purpose" test because it looks only at causal connection, and not a "primary" reason. *See Visa U.S.A., Inc. v. First Data Corp*., No. C-02-1786JSW(EMC), 2004 WL 1878209, at *4 (N.D. Cal. Aug. 23, 2004).

13 F.4th at 714.

breach under the driving force test, although the court's suggestions are not entirely practical.

In that case, the court found that non-litigation concerns were the driving force for commissioning the Mandiant report because Capital One had entered into a Master Services Agreement (MSA) with FireEye years earlier and had entered into periodic Statements of Work (SoW) and purchase orders with Mandiant for various reports during that time. As a financial institution that stores financial and other sensitive information, Capital One, according to its own submission to the court, needed to be positioned to immediately respond to any potential compromise. A key purpose of the MSA and SOWs was to ensure that, in the event of a cybersecurity incident, Capital One could respond quickly. To that end, the SOWs directed Mandiant to provide incident response services, which were broadly characterized as computer security incident response support; digital forensics, log, and malware analysis support; and incident remediation assistance. In addition, under the SOWs, Mandiant was to provide a final report covering these issues and should one be necessary, a written technical document outlining the results and recommendations for remediation. Capital One paid Mandiant for this work from a Capital One fund denominated "business critical" expenses.

When Capital One experienced a security breach on July 20, 2019, it retained outside litigation counsel to provide legal advice, which in turn retained Mandiant pursuant to a Letter Agreement that provided that Mandiant would provide services and advice "as directed by counsel" in the areas of (1) computer security incident response; (2) digital forensics, log, and malware analysis; and (3) incident remediation, "reflecting the same scope of work Mandiant had already agreed to provide under the MSA and SOWs."[7] The Letter Agreement also provided that Mandiant would be paid based on the payment terms set out in the 2019 SOW (and in fact Mandiant was paid from a retainer Mandiant had already received from Capital One pursuant to the 2019 SoW).

---

[7] *In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 3470261, at *1 (E.D. Va. June 25, 2020).

Applying the Fourth Circuit's driving force test,[8] the court found that Capital One met the first prong for work product protection—because the Mandiant report had been prepared at a time when litigation was a real likelihood and not merely a possibility—but failed to meet the second prong of the test—whether the document would have been created in essentially the same form in the absence of the litigation—because Judge Trenga concluded that it would have been prepared regardless of whether litigation had been contemplated. The court focused on the fact that, although requested by outside litigation counsel, the Mandiant report was procured pursuant to a Letter Agreement whose scope of services was identical to a prior SoW procured purely for business purposes. The court ruled that—like the defendants in the *Premera*[9] and *Dominion Dental*[10] security breach

---

[8]In determining whether a document was created in anticipation of litigation, and therefore subject to work product protection, a court in the Fourth Circuit must determine if the document was prepared "because of the prospect of litigation when the preparer faces an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation." *National Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co*., 967 F.2d 980, 984 (4th Cir. 1992) (emphasis added). Where the relevant document may be used for both litigation and business purposes, the court must determine "the driving force behind the preparation of" the requested document. *Id*. at 984. In the Eastern District of Virginia, courts apply a two-pronged test, focusing on (1) whether the document at issue was created when litigation was a real likelihood, and not merely a possibility, and (2) whether the document would have been created in essentially the same form in the absence of litigation. *In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 3470261, at *3 (E.D. Va. June 25, 2020).

[9]*In re Premera Blue Cross Customer Data Security Breach Litig*., 296 F. Supp. 3d 1230, 1245 (D. Or. 2017) (denying work product protection to a Mandiant report involving a breach discovered while Mandiant was already conducting a review of Premera's data management system, after which it continued its work in investigating the breach, where "[t]he only thing that appear[ed] to have changed involving Mandiant was the identity of its direct supervisor, from Premera to outside counsel."). *But see In re Premera Blue Cross Customer Data Security Breach Litig*., 329 F.R.D. 656, 666–67 (D. Or. 2019) (holding in a later opinion in the same case that documents evidencing Premera's response to a breach were "not primarily a business function" because such actions "were likely guided by advice of counsel and concerns about potential liability").

In the later opinion in *Premera,* the court also considered a number of documents typically generated in larger security breaches, ruling that drafts of customer service scripts were subject to protection under work product doctrine, but the final versions of the scripts were not protected and were subject to production. The court also held that a timeline pre-

cases—Capital One had failed to establish, that the report Mandiant would have created for Capital One pursuant to its pre-data breach SoW would not have been substantially the same in substance or scope as the report Mandiant in

---

pared by in-house counsel relating to remediation efforts was not protected by attorney-client privilege or work product doctrine and that investigations by a third party provider into the cause of the data breach and of the company's physical security were not protected as work product. The court also ruled that documents containing edits by counsel were protected by attorney-client privilege, writing that "[w]hen a client sends a draft disclosure document to an attorney for comment or input, the attorney-client privilege attaches to the draft and remains intact even after the final document is disclosed." *In re Premera Blue Cross Customer Data Security Breach Litig*., 329 F.R.D. 656, 662 (D. Or. 2019).

With respect to its different treatment of documents relating to the investigation, the court explained:

> It may well be that counsel will use the results of the audits and investigations "as necessary" in providing legal advice. That does not mean, however, that the primary purpose of the audits or investigations is legal instead of business. For example, Plaintiffs note that the 2013 and 2014 technology audits have been withheld by Premera under this same claim of privilege. The 2013 audit was performed before the data breach occurred and the 2014 audit before the breach was discovered. These audits thus are normal business functions performed on a regular basis, to enable Premera to assess the state of its technology and security. Premera cannot shield them from discovery by delegating their supervision to counsel. . . .
>
> Regarding Premera's investigation into the cause of the breach, discovering how the breach occurred was a necessary business function regardless of litigation or regulatory inquiries. Premera needed to conduct an investigation as a business in order to figure out the problem that allowed the breach to occur so that Premera could solve that problem and ensure such a breach could not happen again. Accordingly, the Court finds that Premera's investigation into the breach was conducted primarily for a business purpose.
>
> If, however, an attorney took the information from these documents and drafted a different document in preparation for litigation, that document would be protected. Additionally, just because an underlying audit or investigatory report is not privileged, an email to an attorney seeking legal advice regarding the report would be privileged and could be redacted. A draft report sent to counsel seeking legal advice and input on the draft also would be privileged.

Id. at 666-67. A different case would be presented if immediately upon discovery of an incident (and not as a normal business audit, as in *In re Premera*), a company conducted a specific and targeted investigation into the incident at the direction of its attorneys so that the company's attorneys could provide advice and protect the company's interests in anticipated litigation. A different case also would be presented if counsel were involved to develop a potential criminal case against the bad actor(s) who accessed its systems.

[10] *In re Dominion Dental Services USA, Inc. Data Breach Litigation,* 429 F. Supp. 3d 190, 192-94 (E.D. Va. 2019) (holding that a cybersecurity report was not protected by the work product doctrine where outside counsel had retained Mandiant to prepare the report a year before the breach at issue was discovered).

fact prepared for outside litigation counsel. Because the scope of the engagements was identical, the court held that Capital One had failed to satisfy the "because of" test.[11]

In support of this ruling, the court also cited the post-production distribution of the Mandiant report as probative of the purpose for which it was initially produced. In *Capital One,* the report had been circulated to approximately 50 employees, a corporate governance office general email box, Capital One's Board of Directors, four different regulators, and Capital One's accountant, underscoring—in Judge Trenga's view—Capital One's business need for the report.[12] In short, the Court concluded that:

> Capital One had determined that it had a business critical need for certain information in connection with a data breach incident, it had contracted with Mandiant to provide that information directly to it in the event of a data breach incident, and after the data breach incident at issue in this action, Capital One then arranged to receive through Debevoise [, its outside counsel,] the information it already had contracted to receive directly from Mandiant.[13]

In response to Capital One's objection that the Magistrate Judge's recommendation would result in terrible public policy by incentivizing companies to either (a) forego keeping an incident response vendor on retainer or (b) hire a new, unfamiliar vendor to investigate any incident from which litigation is expected to result, Judge Trenga glibly opined that this "contention ignore[d] the alternatives available to produce and protect work product, either through different vendors, different scopes of work and/or different investigation teams."[14] Needless to say, it may not be practical or efficient to use separate investigative teams or to use a trusted

---

[11]By contrast, in *In re Experian Data Breach Litigation*, SACV 15-01592 AG (DFMx), 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017), the court held that a Mandiant report was entitled to work product protection, where Mandiant's previous work for Experian was separate from the work it did for Experian regarding the particular breach at issue in that case.

[12]*In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 3470261, at *6 & n.6 (E.D. Va. June 25, 2020).

[13]*In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 3470261, at *7 (E.D. Va. June 25, 2020).

[14]*In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 3470261, at *7 n.8 (E.D. Va. June 25, 2020). The court noted in a different part of the opinion, for example,

and experienced vendor for some incidents but a different one for breaches likely to lead to litigation. Indeed, security professionals urge companies to plan ahead—to undertake table top exercises and identify and work beforehand with any consultants who will be retained—so that important decisions are not made under incredible time pressure in the face of a security incident and the short time deadlines under the GDPR or other legal regimes to provide notice to consumers and regulators. Ultimately, the *Capital One* opinion underscores the risks associated with generating forensic reports (as opposed to mere investigations) and the benefits of retaining special forensics consultants exclusively for litigation.

In a later opinion in the same case, the court upheld the privilege with respect to a report prepared by PricewaterhouseCoopers.[15] While the court's order does not elaborate on the basis for the ruling, the parties' briefs, which were referenced by Magistrate Judge Anderson as having been relied upon by him, make clear that the court was satisfied that the PricewaterhouseCoopers Report had been prepared for litigation and met the "but for" test.

Other courts have both preserved[16] or rejected[17] assertions of work product protection for security incident reports in cybersecurity litigation.

---

that in *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14–2522 (PAM/JJK), 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015), the court upheld Target's assertion of work product protection over a third-party firm's investigation where Target performed its own independent investigation, which was produced, and its attorneys performed a separate investigation through a retained consulting expert, which was protected.

[15] *In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 5016930 (E.D. Va. Aug. 21, 2020).

[16] *See, e.g.*, *In re Experian Data Breach Litigation*, SACV 15-01592 AG (DFMx), 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017) (holding that a Mandiant report was entitled to work product protection); *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14–2522 (PAM/JJK), 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015) (upholding Target's assertion of work product protection); *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190-95 (M.D. Tenn. 2014) (granting a protective order to protect a Stroz Friedberg report prepared in response to a data breach as work product (and attorney-client privileged) where there was no showing that the information sought could not be obtained through other means).

[17] *See, e.g.*, *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7 (D.D.C. 2021) (holding that a Duff & Phelps Report and associated materials were neither protected work product nor attorney-client privileged and had to be produced to the plaintiff in litigation).

In those instances when a report must be generated, there may be other privileges available beyond work product to keep a report confidential. For example, if a non-testifying consultant is retained to investigate a breach, the facts known or opinions held by the consultant are not discoverable absent "exceptional circumstances under which it is impracticable for the party to obtain facts or opinions on the same subject by other means."[18] Relying on other privileges and litigation protections is also a way to sidestep the application of the driving force test in those courts where it may be applied. While often less contentious, confidentiality issues frequently arise in cybersecurity breach cases. Parties typically enter into two-tier stipulated protective orders allowing information to be designated as confidential (with access limited to review by the parties and their counsel and consultants or some other enumerated list of approved recipients) and highly confidential (with access limited typically to just outside counsel or outside counsel and consultants).[19]

---

[18]Fed. R. Civ. Proc. 26(b)(4)(D)(ii); *In Re Marriott International Inc. Customer Data Security Breach Litigation*, MDL No. 19-MD-2879, 2021 WL 2910541 (D. Md. July 12, 2021) (declining to compel production of (1) agreements and statements of work between Marriott and CrowdStrike, (2) all investigations, reports, findings, conclusions, and recommendations made by CrowdStrike, (3) all communications between CrowdStrike and Marriott, (4) all communications between CrowdStrike and Marriott employees concerning the investigations CrowdStrike conducted, or (5) all memoranda, notes, and communications prepared by Marriott's employees reflecting conversations between CrowdStrike and Marriott, where CrowdStrike was retained as a non-testifying consultant within the meaning of Rule 26(b)(4)(D)); *Genesco, Inc. v. Visa U.S.A., Inc*., 302 F.R.D. 168, 189-90 (M.D. Tenn. 2014) (upholding the confidentiality of a Stroz Friedberg report prepared in response to a data breach).

[19]*See, e.g.*, *Layne Christensen Co. v. Purolite Co.*, 271 F.R.D. 240271 F.R.D. 240, 246-47 (D. Kan. 2010) (approving a two tier protective order over plaintiff's objection), *citing among other cases Bittaker v. Woodford*, 331 F.3d 715, 726 (9th Cir. 2003) ("Courts could not function effectively in cases involving sensitive information—trade secrets, medical files and minors, among many others—if they lacked the power to limit the use parties could make of sensitive information obtained from the opposing party by invoking the court's authority."). Two tier protective orders have been approved in putative cybersecurity breach class action suits. *See, e.g.*, *In re: Yahoo! Customer Data Security Breach Litigation*, Case No. 5:16-md-02752-LHK (N.D. Cal.) (ECF No. 73); *In re Anthem, Inc. Data Breach Litigation*, Case No. 5:15-md-02617-LHK (N.D. Cal.) (ECF No. 293). Proposed stipulations limiting access to and use of confidential information are analyzed in chapter 10 in connection with trade secret protec-

Many protective orders entered in data breach cases include particular procedures for filing material under seal (or challenging confidentiality designations). Filings under seal or in redacted form may require a stipulation from counsel (if unopposed) and the approval of the court (regardless of whether all parties join in a request to seal documents or information). Although there is a general presumption that court filings should be publicly available,[20] the Federal Rules make provision for filings under seal or otherwise limiting public disclosure of confidential material.[21] Among other things, courts have sealed technical records relating to a company's network and security systems in cybersecurity breach and data privacy cases, in recognition that public disclosure could raise competitive concerns, as well as providing a blueprint for potential hackers.[22]Data breach cases also may involve discovery requests for laptops

---

tion. Sample forms are reproduced in section 10.16. In many instances, a company will want a two tier protective order, allowing it to designate information as confidential (for review only by the parties and their lawyers and consultants) or attorneys eyes-only.

[20]*See, e.g.*, *Kamakana v. Honolulu*, 447 F.3d 1172, 1178 (9th Cir. 2006) (noting that, subject to exceptions, courts historically have "recognized a 'general right to inspect and copy public records and documents, including judicial records and documents.' *Nixon v. Warner Commc'ns, Inc*., 435 U.S. 589, 597 & n.7 (1978). . . . Parties seeking to seal judicial records bear the burden of overcoming the presumption with 'compelling reasons supported by specific factual findings that outweigh the general history of access and the public policies favoring disclosure.' ").

[21]*See* Fed. R. Civ. Proc. 26(c).

[22]*See, e.g.*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2018 WL 9651897, at *2-3 (N.D. Cal. Jan. 3, 2018) (sealing (1) material relating to "the technology Yahoo uses to provide services and security to its users" which Yahoo argued would allow competitors to "replicate these features and procedures, which could cause competitive harm to Yahoo" and (2) material that if made public "Yahoo contends could lead to another breach in the security of Yahoo's systems" because it contained "detailed information about the technology Yahoo uses to protect its users' information, as well as the methods that were used to breach Yahoo's systems."); *In re Anthem, Inc. Data Breach Litigation*, No. 15-MD-02617-LHK, 2017 WL 9614789, at *2 (N.D. Cal. Aug. 25, 2017) (finding "compelling reasons" to seal, in connection with a motion for preliminary approval of a class action settlement, "confidential information regarding Anthem's information security, including current methods for data security, methods for data security that Anthem intends to implement in the future pursuant to the Settlement Agreement, and specific amounts of funding that Anthem will spend on cybersecurity measure pursuant to the Settlement Agreement" because, with respect to the information security information, "if specific information regarding Anthem's cybersecurity

and mobile devices and account information that, in addition to confidentiality, may raise privacy concerns. Discovery of a plaintiff's mobile device and browsing history may be limited absent a showing of particularized need and proportionality, especially when sought directly (rather than pursuant to a protocol allowing inspection by a third party to preserve the confidentiality of information contained on a laptop or mobile device).[23] Needless to say, this discovery may be obtained

---

practices were disclosed, this could allow cyberattackers greater opportunity to defeat these defenses and substantially harm both Anthem and putative class members."); *In re Google Inc. Gmail Litigation*, Case No.: 13–MD–02430–LHK, 2013 WL 5366963, at *3 (N.D. Cal. Sept. 25, 2013) (sealing parts of plaintiffs' Consolidated Complaint because Google contended that disclosure of the information could cause competitive harm or could adversely affect the security of Gmail; "Google has narrowly tailored its request and has stated compelling reasons to seal portions of the Consolidated Complaint. The first set of materials . . . relates to specific descriptions of how Gmail operates. . . . This information includes the structures that Google has in place and the order in which emails go through these structures. . . . Google contends that if this information were disclosed, competitors would be able to duplicate features of Gmail, which could cause competitive harm to Google. . . . The second set of material . . . concerns information that if made public Google contends could lead to a breach in the security of the Gmail system. . . . Specifically, this material concerns how users' interactions with the Gmail system affects how messages are transmitted. . . . Google contends that hackers and spammers could use this information to circumvent Google's anti-virus and anti-spam mechanisms. . . . The Court credits Google's concern that 'Google's ability to combat spammers, hackers, and others who propagate these unwanted or harmful materials would be impaired if those individuals had visibility into Google's defenses.' "); *see also, e.g.*, *Finjan, Inc. v. Cisco Systems Inc.*, No. 17-CV-00072-BLF, 2019 WL 4168952, at *2 (N.D. Cal. Sept. 3, 2019) (sealing material that "reveals the identification, organization, and/or operation of Cisco's proprietary products," which competitors could "use to map proprietary features of Cisco's products"); *Reyna v. Arris Int'l PLC,* No. 17-CV-01834-LHK, 2018 WL 1400513, at *3 (N.D. Cal. Mar. 20, 2018) (acknowledging that "detailed information about the technology that a company uses to protect against hacking and other types of attacks, or specific vulnerabilities in that technology, is sealable under the compelling reasons standard" but refusing to seal information about a company's internal investigation procedures because disclosure of such "general information" did not present a similar risk).

[23] *See, e.g.*, *Henson v. Turn, Inc.*, Case No. 15-cv-01497-JSW (LB), 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018) (limiting disclosure of browsing history and denying defendant's request to inspect mobile devices in a data privacy case involving alleged "Zombie cookies"; "The undersigned does not mean to imply that there could never be an instance where a request to directly inspect a litigant's electronic devices or forensic im-

upon a proper showing and with adequate protection.[24]

27.07[6] Class Action Settlements in Data Breach Cases

Class action litigation has increased exponentially in recent years with ongoing security breaches, ransomware attacks, state-sponsored cyber-attacks and other incidents, and with the advent of the CCPA[1] and the potential availability of statutory damages. While more cases are being filed, as more security incidents occur, cybersecurity consumer class action litigation today typically does not involve the "pile on" of numerous law firms following news of an incident that was seen in past years, with lawyers filing numerous individual lawsuits around the country, vying for lucrative damage awards from large settlements of cases

---

ages, or a request that a litigant produce his complete web browsing history or cookies, would be relevant and proportional. There may be situations where such a request would be proper, and this order is without prejudice to Turn's renewing its request should such a situation arise."); *In re Anthem, Inc. Data Breach Litigation*, No. 15-md-02617 LHK (NC), 2016 WL 11505231, at *1–2 (N.D. Cal. Apr. 8, 2016) (denying request to inspect or forensically image plaintiffs' computers, tablets, and smartphones as "invad[ing] plaintiffs' privacy interests" and "disproportional to the needs of the case"; "There is an Orwellian irony to the proposition that in order to get relief for a theft of one's personal information, a person has to disclose even more personal information, including an inspection of all his or her devices that connect to the internet. If the Court were to grant [that] request, it would further invade plaintiffs' privacy interests and deter current and future data theft victims from pursuing relief.").

[24]*See, e.g.*, *In re Apple Inc. Device Performance Litigation*, Case No. 5:18-md-02827-EJD, 2019 WL 3973752 (N.D. Cal. Aug. 22, 2019) (allowing discovery of mobile devices and account passwords pursuant to a protocol that provided, among other things, that the forensic imaging would be completed by a neutral, third-party computer forensics vendor, which would disclose the names of everyone who examined or handled plaintiffs' devices or information and would execute the Stipulated Protective Order entered in the case, where the devices, their contents, and their passwords would be designated as Highly Confidential—Attorneys' Eyes Only and forensic copies of the devices would not be provided to counsel, but only to outside experts, who in turn would only provide counsel with their analyses and the data underlying their analyses (redacted to the extent possible, to conceal the contents, authors, recipients, and subject-matter of the underlying data (and any associated metadata), or replaced with summary descriptions).

[Section 27.07[6]]

[1]The CCPA is separately analyzed in section 26.13A in chapter 26.

consolidated by the MDL panel[2] (with the lion's share of fees going to designated lead counsel)—except for the very largest, most significant breaches (based on size, dollar value, or the sensitivity of information). Instead, most cybersecurity breaches may generate one lawsuit, or a small number of suits (perhaps consolidated through traditional means), with other lawyers begging off from cases where the time and effort associated with fighting to become lead counsel may not be justified by the ultimate outcome of the case. Although some data breach cases have resulted in large settlements—and large fee awards—many cybersecurity cases settle for small amounts, either in absolute numbers or on a per-claimant basis. There may be several explanations for this.

First, most putative class action suits arising out of security incidents do not involve actual monetary loss by consumers. 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). As underscored in the earlier sections on standing[3] and claims asserted in cybersecurity breach cases,[4] claimants often sue claiming they have lost time as a result of an incident or incurred purely costs to mitigate the risk of future financial fraud or identity theft. Class action settlements therefore have been focused on injunctive relief, non-economic remedies (such as enhanced security), credit monitoring, and *cy pres* awards (although *cy pres* settlements are harder to get

---

[2]*See, e.g.*, *In re: Capital One Customer Data Security Breach Litigation*, 396 F. Supp. 3d 1364 (M.D.L. 2019) (centralizing cases in the Eastern District of Virginia); *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); *see supra* § 27.07[4] (MDL consolidation).

Class certification issues in internet and mobile cases are analyzed more extensively in section 25.07[2] in chapter 25.

[3]*See supra* § 27.07[2].

[4]*See supra* § 27.07[3].

approved[5]), rather than large damage payments to class members. Alternatively, settlements may provide different terms for the small percentage of class members in a typical data breach who experienced an actual financial loss compared to the much larger group of those members who did not.

Second, as discussed in the preceding subsections, because most consumer putative class action suits do not involve substantial out of pocket losses, many data breach cases present complex causation and damage issues, which make the outcome of a case uncertain and costly to litigate. The issues of standing, the difficulty of fitting the facts of a given case into common law and statutory claims, and the problems of proving causation and damage have made class action litigation less lucrative than many plaintiffs' lawyers first imagined—except in large cases or where substantial losses were incurred (which typically occurs more frequently in business vs. business litigation, apportioning liability, for example, over fraudulent credit card charges, than in consumer class action cases).

Third, while the potential availability of statutory remedies, such as under the CCPA, may increase the settlement value of a case to plaintiffs' counsel, the widespread use of arbitration provisions in consumer contracts may depress the value of a case by an even greater margin in cases where there is privity of contract and an enforceable agreement. The use of arbitration clauses to thwart cybersecurity class action litigation is addressed in section 27.07[7].

Fourth, even if a security incident is common to the class, class certification may not be appropriate because the impact on class members, if any, may require individualized proof—especially causation and harm (or injury) where the putative

[5]The propriety of *cy pres* awards in cases involving broad releases but no payments to class members has been called into question by Chief Justice Roberts and Justice Thomas, but the Supreme Court has not yet had occasion to rule definitely on their propriety. *See Frank v. Gaos*, 139 S. Ct. 1041, 1047-48 (2019) (Thomas, J. dissenting); *Marek v. Lane*, 571 U.S. 1003 (2013) (Statement of Roberts, C.J.); *see also In Re Google Inc. Cookie Placement Consumer Privacy Litigation*, 934 F.3d 316, 321, 325-32 (3d Cir. 2019) (vacating and remanding a *cy pres*-only 23(b)(2) settlement in a data privacy case); *see generally supra* § 25.07[2] (analyzing the propriety of *cy pres*-only settlements).

class has not suffered a common monetary injury.[6]

Fifth, data about prior class action settlements can influence future settlements. Hence, when Target was the largest consumer class action settlement at approximately $10 million (exclusive of attorneys' fees), parties argued in mediation over why their cases were similar to or less significant than that data breach. While there have been much higher settlements since that time, they typically occurred in large breaches involving sensitive financial information or medical

---

[6] *See, e.g.*, *McGlenn v. Driveline Retail Merchandising, Inc.*, No. 18-cv-2097, 2021 WL 165121, at *8-10 (C.D. Ill. Jan. 19, 2021) (denying class certification in a data breach case where a Payroll Department employee of the defendant responded to a phishing scam by sending 15,878 2016 W-2 forms to a scammer posing as Driveline's CFO, which contained sensitive personally identifiable information (PII), including names, mailing addresses, Social Security numbers, and wage and withholding information, for lack of commonality due to individualized issues of causation, injury and damage); *Opperman v. Kong Technologies, Inc.*, Case No. 13-cv-00453-JST, 2017 WL 3149295 (N.D. Cal. July 25, 2017) (denying class certification in an invasion of privacy case alleging that Apple had misrepresented the security features on some of its devices, because plaintiffs could not show that common issues predominated over individual questions or provide a feasible way of measuring damages; "Plaintiffs have not shown that class members saw, heard, or relied upon representations about the specific security features—sandboxing and the Curated App Store—at issue in the case."); *Dolmage v. Combined Insurance Company of America*, No. 14 C 3809, 2017 WL 1754772 (N.D. Ill. May 3, 2017) (denying certification of a putative class of Dillard's employees whose personal information was accessed when an employee of the defendant posted it on defendant's website without adequate security protections where, among other things, the types and amount of damages suffered by putative class members varied widely); *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 293 F.R.D. 21, 31-33 (D. Me. 2013) (denying plaintiffs' motion for class certification in a cybersecurity breach case for failure to establish that common questions predominated over individual issues, where plaintiffs failed to present expert testimony showing that damages could be proven on a class-wide basis at trial. "Without an expert, they cannot prove total damages, and the alternative (which even they do not advocate) is a trial involving individual issues for each class member as to what happened to his/her data and account, what he/she did about it, and why.").

While plaintiffs typically seek certification on the issue of liability, which defendants typically oppose, when a case settles, defendants may want certification of a settlement class to maximize the preclusive effect of any settlement and extinguish claims of putative class members (other than those who affirmatively opt out).

Certification issues are analyzed more extensively in section 25.07[2] in chapter 25 (class certification in internet cases) and 26.15 in chapter 26 (data privacy litigation).

information. Ultimately, class action settlements are all over the map[7] with the largest ones gaining the most publicity,

[7]*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 Equifax Inc. Customer Data Security Breach Litigation*, 999 F.3d 1247 (11th Cir. 2021) (affirming certification of a settlement class and final approval of a settlement that included a settlement fund of $380.5 million and a fee award of $77.5 million (or 20.36% of the value of the fund, excluding any additional contributions that Experian might be required to make under the terms of the settlement) plus $1,404,855.35 in expenses, but narrowly reversing and remanding service awards of $2,500 per person to each of the named class representatives); *In re Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 16-MD-02752-LHK, 2020 WL 4212811 (N.D. Cal. July 22, 2020) (certifying a settlement class comprised of approximately 194 million people and granting final approval to a class action settlement valued at $117 million (or roughly 60.3 cents per class member), including $22,763,642.70 in attorneys' fees (or 25.5% of the fund), $1,477,609.54 in unreimbursed costs and expenses, $60,000 in cost reserve for retention of a cybersecurity expert, and $87,500 in service awards (at $2,500, $5,000 and $7,500 per person for different class representatives)); *Gordon v. Chipotle Mexican Grill, Inc.*, Civil Action No. 17-cv-01415-CMA-SKC, 2019 WL 6972701 (D. Colo. Dec. 16, 2019) (certifying a settlement class and granting final approval to a settlement to a cybersecurity suit where roughly 10 million payment cards may have been affected by the security incident and a total of 6,429 claims were timely submitted, awarding $1,200,000.00 in fees and $2,500 per person in service awards); *In re Sonic Corp. Customer Data Security Breach Litigation*, MDL No. 2807, 2019 WL 3773737 (N.D. Ohio Aug. 2019) (certifying a settlement class and granting final approval to a class action settlement creating a non-reversionary $4,325,000 aggregate fund, awarding attorneys' fees of $1,297,500 (30% of the aggregate value of the settlement), $209,536.76 in costs and expenses, and approving service awards ranging from $1,000 to $5,500 for each of 13 class representatives); *In re Premera Blue Cross Customer Data Security Breach Litigation*, Case No. 3:15-md-2633-SI, 2019 WL 3410382 (D. Or. July 29, 2019) (granting preliminary approval to a proposed $32 million settlement to fund a non-reversionary Qualified Settlement (with a minimum of $10 million to be paid as compensation to class members), in a suit arising from a breach that allegedly compromised the confidential information of approximately 11 million current and former members, affiliated members, and employees of Premera); *In re Arby's Restaurant Group, Inc. Data Security Litigation*, Case No. 1:17-mi-55555-

but the numbers are often smaller in other cases (and, on a per-claimant basis, awards, even in some of the larger settlements, have been modest,[8] although parties often focus on

---

WMR, 2019 WL 2720818 (N.D. Ga. June 6, 2019) (granting final approval to a settlement that included a "total potential benefit to the class" of up to $3,306,000, and awarding $4,500 in service awards for each class representative, $35,000 in costs and expenses, and $980,000 in attorneys' fees (approximately 30% of the total fund)); *In re Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 16-MD-02752-LHK, 2019 WL 387322 (N.D. Cal. Jan. 30, 2019) (denying preliminary approval of a proposed class action settlement); *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299 (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), *appeals dismissed*, Nos. 18-16866, 18-16826, 2018 WL 7890391, 2018 WL 7858371 (9th Cir. Oct. 15 & 17, 2019); *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), *aff'd in part, vacated in part*, 931 F.3d 1065 (11th Cir. 2019) (vacating the district court's $15.3 million fee award, which had been based on a lodestar calculation multiplied by 1.3 because it was an abuse of discretion to use a multiplier to account for risk in a fee-shifting case); *In re the Home Depot, Inc*., Case No.: 1:14-md-02583-TWT, 2020 WL 415923 (N.D. Ga. Jan. 23, 2020) ordering, on remand from the Eleventh Circuit, that Home Depot pay to plaintiffs' counsel, in accordance with the terms of the settlement agreement, the sum of $14,532,418.31 in attorneys' fees and $731,986.71 in expenses); *In re The Home Depot, Inc. Customer Data Security Breach Litigation*, No. 14-MD-02583-TWT, 2016 WL 6902351, at *7 (N.D. Ga. Aug. 23, 2016) (granting final approval of $28.4 settlement to consumer class of roughly 52 million (or roughly 55 cents per class member)); *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 cardholders 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).

[8] As one court acknowledged in preliminarily approving a $32 million proposed settlement of a class of 10.6 million potential claimants (which only guaranteed a minimum of $10 million in payment to class members), while analyzing the benefits of settlement beyond merely financial compensation and the risks associated with litigation:

> The Court recognizes that a guarantee of no less than $10 million to be spent on the recovery of a class of potentially 10.6 million people may seem low. The reality, however, is that through the time of the briefing on class certification, it does not appear that the percentage of Class Members who suffered actual

the expected payout to class members who meet the eligibility requirements to submit a valid claim, rather than per-class member averages).

For example, the following are statistics from some of the better publicized security breach class action settlements, showing the dates, settlement amounts ultimately approved, and courts that granted approval:

- *In re Equifax Inc. Customer Data Security Breach Litigation*, 999 F.3d 1247 (11th Cir. 2021) (affirming certification of a settlement class and final approval of a settlement that included a settlement fund of $380.5 million and a fee award of $77.5 million (or 20.36% of the value of the fund, excluding any additional contributions that Experian might be required to make under the terms of the settlement) plus $1,404,855.35 in expenses, but narrowly reversing and remanding service awards of $2,500 per person to each of the named class representatives, in a class estimated to include 147 million members). The settlement also included a complex series of provisions, making a per-claimant calculation difficult to estimate precisely.[9]
- *In re Wawa, Inc. Data Security Litigation*, Civil Action No. 19-6019, 2021 WL 3276148 (E.D. Pa. July 30, 2021)

---

identity theft, and therefore would be eligible for the out-of-pocket reimbursement, is very large. The Court also recognizes that even assuming that no Class Member suffered identity theft that could plausibly be traced to the Data Breach, the default settlement of $50 would only allow for recovery by 130,000 Class Members.

In re Premera Blue Cross Customer Data Security Breach Litigation, Case No. 3:15-md-2633-SI, 2019 WL 3410382, at *22 (D. Or. July 29, 2019).

[9]The settlement included:

- Reimbursement for up to $20,000 of documented, out-of-pocket losses fairly traceable to the data breach (*e.g.*, the cost of freezing a credit file, professional fees due to identity theft);
- Compensation of $25 per hour for up to 20 hours (subject to a $38 million cap) for time spent taking preventative measures or dealing with identity theft, with no documentation needed for the first 10 hours;
- Four years of three-bureau credit monitoring and identity protection services through Experian;
- An additional six years of one-bureau credit monitoring and identity protection services through Equifax, which will be provided separately by Equifax and not paid for from the settlement fund;
- Alternative cash compensation (subject to a $31 million cap) for class members who already have credit monitoring and who do not wish to enroll in the settlement's programs;[4] and

(granting preliminary approval to a consumer class action settlement providing reimbursement or gift cards to those who could show actual harm and injunctive relief, in a case where the information of up to 22 million customers potentially were put at risk).[10]

- *Atkinson v. Minted, Inc.,* Case No.: 3:20-cv-03869-VC, 2021 WL 2411041 (N.D. Cal. May 14, 2021) (granting preliminary approval to a $5 million settlement of California Consumer Privacy Act and other claims brought on behalf of a class of 4.1 million people whose names, email addresses, hashed and salted passwords, and, for those who provided this information, telephone numbers, billing addresses, shipping addresses, and for some affected customers, birthdates, were subject to a security incident); *see also Atkinson v. Minted, Inc*., Case No.: 3:20-cv-03869-VC, 2021 WL 6028374 (N.D. Cal. Dec. 17, 2021) (granting final approval).
- *In re Google Plus Profile Litigation*, Case No. 5:18-cv-06164-EJD (VKD), 2021 WL 242887 (N.D. Cal. Jan. 25, 2021) (granting final approval to settle claims arising from software bugs between 2015 and 2018 that allegedly allowed app developers to access Google+ profile field information of 500,000 class members in an unintended manner, for $7.5 million, or approximately

---

- Seven years of identity restoration services through Experian to help class members who believe they may have been victims of identity theft.

Beyond these class benefits, Equifax agreed to pay an additional $125 million if needed to satisfy claims for out-of-pocket losses and potentially $2 billion more if all 147 million class members sign up for credit monitoring. In no circumstance would money in the settlement fund revert back to Equifax. Instead, if money remained in the settlement fund after the claim periods, the settlement provides ways in which the above class benefits would be increased. Equifax also was required to spend a minimum of $1 billion on data security over five years and to comply with certain data security requirements, to be audited by an independent assessor and subject to the district court's enforcement powers. *See In re Equifax Inc. Customer Data Security Breach Litigation*, 999 F.3d 1247, 1257-59 (11th Cir. 2021).

[10]The suit arose after hackers hijacked Wawa, Inc. customer payment card information beginning in March 2019 and continuing over the next several months. The hackers allegedly accessed Wawa's point-of-sale systems and installed malware that targeted in-store payment terminals and gas station fuel dispensers, harvesting information that was allegedly made available for purchase on the dark web.

The breach resulted in litigation by consumers, financial institutions, and employees.

$15 per class member, from which the court awarded $1,875,000.00 in attorneys' fees and costs and $69,558.23 in litigation expenses).

- *In re Yahoo! Inc. Customer Data Security Breach Litigation*, Case No. 16-MD-02752-LHK, 2020 WL 4212811 (N.D. Cal. July 22, 2020) (certifying a settlement class comprised of approximately 194 million people and granting final approval to a class action settlement valued at $117 million (or roughly 60.3 cents per class member), including $22,763,642.70 in attorneys' fees (or 25.5% of the fund), $1,477,609.54 in unreimbursed costs and expenses, $60,000 in cost reserve for retention of a cybersecurity expert, and $87,500 in service awards (at $2,500, $5,000 and $7,500 per person for different class representatives)).
- *In re Hanna Andersson and Salesforce.com Data Breach Litigation*, Master File No. 3:2020-cv-00812-EMC, 2020 WL 10054678 (N.D. Cal. Dec. 29, 2020) (preliminarily approving claims arising from a breach in which hackers accessed customers' names, billing and shipping addresses, payment card numbers, CVV codes, and credit card expiration dates of approximately 200,273 individuals for $400,000, or approximately $2 per class member).
- *Carroll v. Macy's, Inc.*, No. 2:18-cv-01060, 2020 WL 3037067 (N.D. Ala. June 5, 2020) (certifying a settlement class and granting final approval to the settlement of claims arising from a 2018 data breach that exposed online customer profiles of 163,000 class members and personal information associated with those profiles for $192,500, or approximately $1.18 per class member).
- *Gordon v. Chipotle Mexican Grill, Inc*., Civil Action No. 17-cv-01415-CMA-SKC, 2019 WL 6972701 (D. Colo. Dec. 16, 2019) (certifying a settlement class and granting final approval to a settlement to a cybersecurity suit where roughly 10 million payment cards may have been affected by the security incident and a total of 6,429 claims were timely submitted, awarding $1,200,000.00 in fees and $2,500 per person in service awards).
- *In re Sonic Corp. Customer Data Security Breach Litigation*, MDL No. 2807, 2019 WL 3773737 (N.D. Ohio Aug. 2019) (certifying a settlement class and granting final approval to a class action settlement creating a non-reversionary $4,325,000 aggregate fund, awarding attorneys' fees of $1,297,500 (30% of the aggregate value

of the settlement), $209,536.76 in costs and expenses, and approving service awards ranging from $1,000 to $5,500 for each of 13 class representatives).

- *In re Premera Blue Cross Customer Data Security Breach Litigation*, Case No. 3:15-md-2633-SI, 2019 WL 3410382 (D. Or. July 29, 2019) (granting preliminary approval to a proposed $32 million settlement to fund a non-reversionary Qualified Settlement (with a minimum of $10 million to be paid as compensation to class members), in a suit arising from a breach that allegedly compromised the confidential information of approximately 11 million current and former members, affiliated members, and employees of Premera).
- *In re Arby's Restaurant Group, Inc. Data Security Litigation*, Case No. 1:17-mi-55555-WMR, 2019 WL 2720818 (N.D. Ga. June 6, 2019) (granting final approval to a settlement that included a "total potential benefit to the class" of up to $3,306,000, and awarding $4,500 in service awards for each class representative, $35,000 in costs and expenses, and $980,000 in attorneys' fees (approximately 30% of the total fund)).
- *In re Anthem, Inc. Data Breach Litigation*, 327 F.R.D. 299 (N.D. Cal. 2018), *appeals dismissed*, Nos. 18-16866, 18-16826, 2018 WL 7890391, 2018 WL 7858371 (9th Cir. Oct. 15 & 17, 2019) (settling claims against Anthem arising from a 2015 data breach of the private health information of 79.15 million customers for $115 million, or approximately $1.45 per class member).
- *In re Target Corp. Customer Data Security Breach Litigation,* 892 F.3d 968 (8th Cir. 2018) (affirming approval of a settlement arising out of the 2013 data breach of the payment card information of 100 million U.S. customers, for $10 million, or approximately $0.10 per class member, and a separate award of expenses and fees to class counsel of $6.75 million, for an effective rate of $0.16775 per class member, over objections that the district court awarded "worthless objective relief," inadequately compensated class members, and ignored "subtle signs of collusion" based on ostensible clear-sailing and kicker provisions[11]).

---

[11]*See In re Target Corp. Customer Data Security Breach Litigation,* 892 F.3d 968, 979 (8th Cir. 2018) ("A clear-sailing provision is one where 'the defendants agree[ ] not to oppose the request for attorney fees,'

- *In re The Home Depot, Inc. Customer Data Security Breach Litigation*, No. 14-MD-02583-TWT, 2016 WL 6902351, at *7 (N.D. Ga. Aug. 23, 2016) (granting final approval of $28.4 settlement to consumer class of roughly 52 million (or roughly 55 cents per class member).[12]
- *In re: LinkedIn User Privacy Litigation*, 309 F.R.D. 573 (N.D. Cal. 2015) (approving settlement of claims arising from a 2012 data breach of 6.5 million LinkedIn passwords for $1.25 million, or approximately $0.19 per class member, and awarding 25% or $312,500 in in attorneys' fees and $26,608.67 in expenses, where the parties estimated that class members who submitted valid claims would each receive $14.81, or roughly 30% of what they could hope to recover at trial).
- *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, No. 11-md-2258 (S.D. Cal. May 4, 2015) (entering final judgment and awarding $2.75 million in attorneys' fees); *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, No. 11-md-2258 (S.D. Cal. July 10, 2015) (granting preliminary approval to settlement of claims arising out of a 2011 breach on Sony Corp. that allegedly exposed 77 million user accounts on the PlayStation Network, including credit card information, for $15 million in games, online currency and identity theft reimbursement to PlayStation Network users affected by a massive 2011 Sony Corp. data breach, or approximately $0.19 per class member based on the original estimate of the value of the settlement (and excluding attorneys' fees and costs)).
- *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*, 851 F. Supp. 2d 1040 (S.D. Tex.

Johnston v. Comerica Mortg. Corp., 83 F.3d 241, 243 (8th Cir. 1996), and a kicker provision means that unused assets from the settlement are returned to the defendants instead of being distributed to the class, *In re Bluetooth Headset Prods. Liab. Litig.*, 654 F.3d 935, 947 (9th Cir. 2011). . . . Sciaroni's position simply voices generalized grievances with these provisions: nowhere does he explain *how* the clauses, even assuming they are present, operated to the detriment of the class.").

[12]In a separate action brought by banks, the court approved a $42.5 million common fund settlement, and plaintiffs' counsel were awarded $11.733 million. in legal fees. *See Northeastern Engineers Federal Credit Union v. Home Depot, Inc.,* No. 20-10667, 2022 WL 40210 (11th Cir. Jan. 5, 2022).

2012) (certifying a settlement class in a suit by credit cardholders 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).

These data points, of course, can be deceiving as there is no perfect market for information on resolution of putative data security breach class action litigation. For example, settlement statistics don't reflect the number of cases won by defendants, dropped by plaintiffs without payment, or settled confidentially on an individual basis. In addition, no two cases are identical in terms of a defendant's potential exposure and wrongdoing, if any, and the strength or weakness of a plaintiff's claims. Further, apple-to-apple comparisons are hard to make when non-economic settlement terms (and even some of the economic terms) vary widely from settlement to settlement. The size of a class isn't always known with precision, which adds to the imprecision. It is also difficult to compare a claims-made settlement, where a defendant only pays for the claims submitted (potentially without a cap) from a settlement where a defendant pays a lump sum that will be divided among claimants regardless of the number of claimants who submit claims. Even for common fund classes, dividing the fund by the number of claimants (or dividing the net amount remaining for the class, after fees and costs are paid out, by the total class size) typically produces a per-class member number that is lower than what is actually paid out due to the relatively small percentage of putative class member who submit claims in connection with cybersecurity data breach class action settlements and eligibility requirements to obtain payments (which vary from settlement to settlement, or even within a given settlement where different users are not similarly situated). Breaches that compromise credit card information also frequently involve parallel consumer and bank/financial institution class action suits,[13] such that the total amount paid in one settlement may not reflect the

[13] *See, e.g.*, *In re the Home Depot, Inc*., Case No.: 1:14-md-02583-TWT, 2020 WL 415923 (N.D. Ga. Jan. 23, 2020) (awarding fees, on remand, in the financial institutions class action suit against Home Depot, arising out of the same security breach for which a consumer class action settlement

actual cost to the company. Among other factors that may influence the amount of a settlement are:

- ***Plaintiff's counsel and the number of plaintiff's counsel involved***. Experienced class action litigators may have a clearer sense of the value of a case. Busy lawyers may be more willing to offload a weak case (or one which could require extensive work with an unclear outcome). Hungrier lawyers may be more willing to "roll the dice" on a large outcome or more willing to accept a small payout than lawyers with a heavy caseload. Class action lawyers who handle many breach cases may be unwilling to impact what they perceive as "the market value" of a settlement, whereas lawyers with a varied practice may be less concerned about how one settlement could impact other cases. When multiple firms are involved, it may take more money to convince them to settle, then when only one firm will get the fee.
- ***The procedural posture of the case, the claims asserted, and whether plaintiffs' claims are subject to arbitration.*** If putative class members are bound by arbitration agreements, this may depress the settlement value of a case for plaintiffs. If statutory damages or attorneys' fees are potentially available, that could enhance plaintiffs' counsel's expectations. If causation and damages are unique to class members, plaintiffs may have a tougher time certifying a liability class, which could depress the value of a case.[14] The procedural posture of a case at the time of settlement may also impact the amount of the settlement. Depending on the parties involved and their respective interests, defen-

---

had previously been reached); *In re Sonic Corp. Customer Data Security Breach Litigation (Financial Institutions)*, Mdl No. 2807, 2020 WL 3577341 (N.D. Ohio July 1, 2020) (granting in part, denying in part, defendant's motion to dismiss putative class claims brought by banks arising out of the same data breach where a consumer class action settlement had been approved the year before); *See In re Equifax Inc., Customer Data Security Breach Litigation*, 371 F. Supp. 3d 1150 (N.D. Ga. 2019) (granting in part, denying in part, defendant's motion to dismiss plaintiffs' claims in a putative class action suit brought by financial institutions, which alleged they were forced to expend resources to assess the impact of the *Equifax* breach).

[14]Those potential obstacles to certification of a liability class may not be present if the plaintiffs seek certification of a settlement class because causation and damage typically need not be proven (or can be resolved through an agreed-upon claims process).

dants may be willing to pay, and plaintiffs willing to accept, different amounts based on their perception of future costs and efforts saved by the settlement. On the other hand, if many of plaintiffs' claims have been eliminated through motion practice, the case may be positioned to settle for less. If a case has already been certified as a class action, plaintiffs may seek more to settle. If the motion has not yet been filed, they may be willing to accept less given the uncertainties associated with litigation.

- ***Defense counsel and their experience with the subject matter, technology and type of case.***
- ***Defendant's culpability, reputation and business objectives.*** If the defendant is motivated to settle for business reasons unrelated to the litigation, this could impact the final settlement terms. Likewise, if the defendant is a likely target of other class action litigation, it may be reticent to "overpay" in a given case, so as not to create an incentive for class action lawyers to target it for future litigation. Defendants who have been subject to multiple cybersecurity breaches may end up paying more than companies that have experienced their first data breach.
- ***The availability of insurance coverage or indemnification and the financial condition of the defendant.*** The availability and extent of insurance coverage may increase or depress the amount of a settlement, depending on the financial solvency of the defendant and its willingness to fight, among other things. A startup company with limited insurance may be able to settle a case for less than a Fortune 100 company with ample insurance coverage. The potential availability of indemnification may also impact the amount of a settlement.
- ***The skill and past experience of the mediator.*** As with lawyers, some mediators are simply better than others. Some have a keener understanding of how a given case would play out in litigation than others. Many are influenced by their prior experience.
- ***Data on past settlements and the terms that the assigned judge would likely approve.*** Data from prior cybersecurity breach class action suits may inform discussions in a given case, either in absolute or per-class member terms. Local and applicable circuit and

district court law and preferences also may impact a settlement. For example, the Northern District of California has guidelines for approving class action settlements.[15] Knowing that the assigned judge has approved—or rejected—particular settlement terms may inform how a settlement is framed.

While no two data breach cases are identical, plaintiffs' class action lawyers typically look to other recent settlements to evaluate the basis for settling a given case. In general, settlements may be higher overall where sensitive information has been breached (such as personal healthcare information, or financial information that could be used to identity theft or other financial fraud), where consumers have been financially harmed, and where the class size is large. A major factor in many cases is the absence of monetary harm and, even in instances where there has been identity theft or financial harm, the complexity of proving causation, where a given putative class may have had their information exposed multiple timesin separate incidents[16]—or even in the same incident.[17] Other factors that may impact the value of a settlement include the underlying merits, the claims asserted and whether plaintiffs could be entitled to recover statutory damages and/or attorneys' fees, whether some or all class members are bound by arbitration agreements (which would put downward pressure on any settlement number), the procedural posture of the case, the trial judge's articulated views in the case, the availability or unavailability of insurance funds, the solvency of the defendant, the strength of the named plaintiffs' individual case (based on the facts alleged or presented), and the approach to settlement of counsel, among other things. Although it can be deceptive to make such comparisons, lawyers and mediators may compare their cases to others that settled, either as an absolute amount or on a per-claimant basis. These numbers, of course, are distorted in

[15] *See Procedural Guidance for Class Action Settlements,* available at: https://www.cand.uscourts.gov/forms/procedural-guidance-for-class-action-settlements/ (last visited June 13, 2021).

[16] Discovery may show that a given plaintiff had the same information—or much worse—exposed in multiple prior incidents.

[17] For example, multiple companies may be sued over the same attack, which caused individual putative class members to be have their information exposed more than once to the same cybercriminals, from the same attack or series of attacks.

that they necessarily do not account for the number of cases where recovery has been zero because the defendants prevailed on the merits or the plaintiffs chose to dismiss their claims.

27.07[7] Business to Business Litigation, Future Trends, Arbitration and Other Class Action Litigation Issues in Data Breach Cases

In contrast to consumers, whose compensable injuries and risk of loss effectively may be 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 example, in *Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*,[1] 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."

Litigation involving risk of loss issues between companies and insurers, credit card companies, banks and merchants, frequently involve higher dollar claims than consumer class actions arising out of a security breach.

[Section 27.07[7]]

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

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. Security breach notification statutes created an incentive for businesses to address security concerns, both for public and customer relations reasons (and because the notice itself potentially may invite attention from regulators and class action lawyers). In addition, as analyzed in section 27.04[6], numerous state statutes now require or create incentives for companies to adopt written information security programs.[2] The growing list of state data security statutes catalogued in other subsections of section 27.04 and California's enactment of the California Consumer Privacy Act,[3] as well as international developments, including in the European Union,[4] have made data security considerations top of mind for inhouse counsel and C level executives, even in companies that themselves may not have designated a formal Chief Information Security Officer (CISO).

The absence of broad safe harbors from litigation 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 putative class action litigation by entering into contracts with binding arbitration provisions[5] (including class action waivers, which outside of arbitration are not necessarily enforceable, depending on the

---

[2] *See supra* § 27.04[6].

[3] *See supra* § 26.13A.

[4] *See supra* §§ 26.04, 26.04A, 26.04B.

[5] *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); *Zheng v. Live Auctioneers LLC*, 20-cv-9744 (JGK), 2021 WL 2043562 (S.D.N.Y. May 21, 2021) (compelling arbitration of claims for negligence and under section 349 of New York's General Business Laws in a putative data breach class action suit); *Hidalgo v. Amateur Athletic Union of United States, Inc.,* 468 F. Supp. 3d 646, 656-58 (S.D.N.Y. 2020) (compelling individual arbitration of plaintiff's putative data breach class action suit, where plaintiff had "reasonable notice" that by completing his application for AAU membership and becoming a member of the AAU, he would be bound by contractual language contained in the documents, including the binding arbitration provision, that could be accessed through the hyperlinks on the AAU application page); *Grice v. Uber Technologies, Inc*., Case No. CV 18-2995 PSG (GJSx), 2020 WL 497487, at *4-11 (C.D. Cal. Jan. 7, 2020) (compelling arbitration of an Uber driver's claims arising out of a 2016 cybersecurity breach and holding that the driver's claim did not come within the exemption created by section 1 of the Federal Arbitration Act for "contracts of employment of seamen, railroad employees, or any other class of workers engaged in foreign or interstate commerce."), *mandamus denied,* 974 F.3d 950 (9th Cir. 2020); *Heller v. Rasier, LLC*, Case No. CV 17-8545 PSG (GJSx), 2020 WL 413243, at *2-9 (C.D. Cal. Jan. 7, 2020) (compelling arbitration of plaintiffs' claims against Uber arising out of an alleged data breach); *In re Uber Technologies, Data Security Breach Litig*., No. CV 18-3169 PSG (GJSx), 2019 WL 6317770 at *2-4 (C.D. Cal. Aug. 19, 2019) (enforcing Uber's ToU, and compelling arbitration of plaintiff's claims arising out of an alleged cybersecurity breach, based on plaintiff's initial assent plus notice of amended Terms and a revised arbitration provision sent by email); *Yu v. Volt Information Sciences, Inc*., Case No. 19-cv-01981-LB, 2019 WL 3503111 (N.D. Cal. Aug. 1, 2019) (compelling arbitration of plaintiff's claims against a former employer, arising out of a data breach, based on the arbitration provision in Yu's employment agreement with Volt); *Gutierrez v. FriendFinder Networks Inc.*, Case No. 18-cv-05918-BLF, 2019 WL 1974900, at *7-8 (N.D. Cal. May 3, 2019) (enforcing the Terms of Use of an adult website, and compelling arbitration, in a cybersecurity breach case, based on plaintiff's actual knowledge of the ToU); *Sultan v. Coinbase, Inc.,* 354 F. Supp. 3d 156, 158-62 (E.D.N.Y. 2019) (compelling arbitration, in a suit brought by a Coinbase account holder alleging negligence where the account holder was contacted by a hacker purporting to be a Coinbase representative, who defrauded the account holder of more than $200,000, using personal information that the plaintiff disclosed during the call, where Coinbase's Disputes Analyst testified that an account could not have been created unless a user filled out all requested information in Coinbase's online form and checked a box certifying that he was 18 years or older and agreeing to Coinbase's User Agreement (which included an arbitration provision) and Privacy Policy, both of which were accessible via a link); *West v. Uber Technologies*, Case No. 18-CV-3001-PSG-GJS, 2018 WL 5848903, at *3-5 (C.D. Cal. Sept. 5, 2018) (enforcing Uber's ToU, and compelling arbitration of plaintiff's claims arising out of an alleged cybersecurity breach, where plaintiff was provided with reasonable notice of the Terms in the form of a clickable gray box and was given notice of the amended Terms and arbitration provision by email and continued to use the app for a year thereaf-

applicable jurisdiction). Because the enforceability of arbitration provisions in consumer cases is hotly contested and subject to a large body of reported case law, a business should be careful to ensure that it enters into a binding contract that contains an enforceable arbitration provision governed by the Federal Arbitration Act (which preempts state law), including a delegation clause to maximize its potential enforceability.[6] Crafting a binding and enforceable arbitration provision is addressed in section 22.05[2][M] in chapter 22, which also includes a sample form. Ensuring that contract formation for online and mobile agreements conforms to the law in those jurisdictions most hostile to electronic contracting is analyzed extensively in section 21.03 in chapter 21.

Where claims arising out of data breach are 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.[7] In the words of one district court judge, that provision "encourages and immunizes content

---

ter); *Patni v. Uber Technologies*, No. CV 18-3002 PSG (GJSx), 2018 WL 5904007, at *2-5 (C.D. Cal. Sept. 5, 2018) (compelling arbitration of plaintiff's cybersecurity breach claims where the plaintiff acknowledged contract formation but argued that the 2016 breach fell outside the scope of the arbitration agreement, and that the agreement was unconscionable, which the court held were issues delegated to the arbitrator); *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).

[6]*See, e.g.*, *Henry Schein, Inc. v. Archer & White Sales, Inc.*, 139 S. Ct. 524, 529 (2019) (holding that "[w]hen the parties' contract delegates the arbitrability question to an arbitrator, a court may not override the contract" and "possesses no power to decide the arbitrability issue . . . even if the court thinks that the argument that the arbitration agreement applies to a particular dispute is wholly groundless"); *Rent-A-Center, West v. Jackson*, 130 S. Ct. 2772 (2010); *see generally supra* § 22.05[2][M].

[7]47 U.S.C.A. § 230(c); *In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1028-35 (N.D. Cal. 2021) (dismissing as precluded by section 230(c)(1) in a putative class action suit, claims for failing to protect the security of Zoom against breaches referred to as "Zoombombing," which allegedly exposed users to harmful third party content, to the extent plaintiffs' claims challenged the harmfulness of

moderation, not security failures."[8] Thus, claims in data breach cases premised on the provision of third party content (or failure to block access to) third party content may be immunized, whereas those that solely involve a defendant's own conduct or content would likely not be immunized.[9]

Analogous litigation issues in data privacy cases are considered in section 26.15 in chapter 26.

27.08 Analysis of State Security Breach Notification Statutes

27.08[1] Overview and Strategic Considerations

All fifty states, the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands have security breach notification statutes in effect.[1] An increasing number of states also have enacted the Insurance Data Security Model Law or otherwise have adopted special security breach provisions for persons and entities licensed, authorized, or registered pursuant to state insurance laws.[2] Financial institutions subject to the Gramm-Leach-Bliley Act may also

---

third party content and derived from defendant's status as publisher or speaker); *see generally infra* § 37.05.

[8] *In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1030-34 (N.D. Cal. 2021). Content moderation is separately analyzed in chapter 49 and multiple other sections of the treatise.

[9] *See generally infra* § 37.05.

[Section 27.08[1]]

[1] A compendium of the security breach notification statutes and implementing regulations enacted as of January 15, 2022 and in effect on that date or thereafter in each state and territory is set forth in section 27.09. Each statutory provision catalogued in section 27.09 identifies its effective date, which is the date it took (or will take) effect (to make it easy for readers to confirm whether a newer version has taken effect between updates).

With the adoption of security breach notification statutes by Alabama and South Dakota in 2018, by July 1 of that year, every state had enacted some form of security breach notification statute.

[2] *See infra* § 27.08[15]. As analyzed in sections 27.04[6][M] and 27.08[15], **Alabama, Connecticut, Delaware, Hawaii, Indiana, Iowa, Louisiana, Maine, Michigan, Minnesota, Mississippi, New Hampshire, North Dakota, Ohio, South Carolina, Tennessee, Virginia,** and **Wisconsin,** have enacted variations of the National Association of Insurance Commissioners' Insurance Data Security Model Law and **Maryland** and **Washington** require notice to their state's respective insurance commissioners of Cybersecurity events. A copy of the Model Law is reproduced in Appendix 11. *See generally infra* § 27.08[15].

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2023

Ian C. Ballon

2023 UPDATES – INCLUDING NEW AND IMPORTANT FEATURES

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator – a 5 volume-set & On Westlaw!

To order call 1-888-728-7677
or visit IanBallon.net

Key Features of E-Commerce & Internet Law

- AI, ML, screen scraping and data portability
- Antitrust in the era of techlash
- The CPRA, Virginia, Colorado and Nevada pricy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- Software copyrightability and fair use after *Google v. Oracle*
- Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- The law of SEO and SEM – and its impact on e-commerce vendors
- Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi,* patentable subject matter, negative trade secrets, rights 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 hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- Enforcing judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Applying the First Sale Doctrine to virtual goods
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & 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
- Click fraud
- Copyright and Lanham Act fair use
- 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/ AI/ 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
- Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

Volume 1

Volume 2

Volume 3

Volume 4

Volume 5

"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 in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.

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 Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

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 selected as the Lawyer of the Year for information technology law in the 2023, 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

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).

Mr. Ballon is also 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.lanBallon.net).

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

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2023

- **Antitrust in the era of techlash** (chapter 34)
- **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurty breach, data privacy, AdTech and TCPA class action suits.**
- **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States,* 141 S. Ct. 1648 (2021)** (ch5)
- **FOSTA-SESTA** and ways to maximize CDA protection (ch 37)
- **IP aspects of the use of #hashtags** in social media (ch 6)
- The **CLOUD Act** (chapter 50)
- **Virginia, Colorado and Nevada privacy laws** (ch 26)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- **Digital economy litigation strategies**
- **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- **Website and mobile accessibility** under the ADA and state laws (chapter 48)
- **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- 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)
- **AdTech law** (chapter 28, Darren Abernethy)
- **The risks of being bound by the CASE Act's ostensibly *voluntary* jurisdiction over small copyright cases**
- **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Idea protection & misappropriation** (ch 13)
- Revisiting **links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- **eSIGN case law** (chapter 15)