SECURITY BREACH CLASS ACTION LITIGATION

Excerpted from Chapter 27 (Internet, Network and Data Security) of
E-Commerce and Internet Law: A Legal Treatise With Forms, Second Edition,
a 4-volume legal treatise by Ian C. Ballon (Thomson/West Publishing 2014)

SANTA CLARA UNIVERSITY LAW PRESENTS

"HOT TOPICS IN INTERNET, CLOUD, AND PRIVACY LAW"

SANTA CLARA UNIVERSITY LAW SCHOOL
APRIL 23, 2015

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:
1900 University Avenue, 5th Fl.
East Palo Alto, CA 914303
Direct Dial: (650) 289-7881
Direct Fax: (650) 462-7881

Los Angeles:
1840 Century Park East
Los Angeles, CA 90067
Direct Dial: (310) 586-6575
Direct Fax: (310) 586-0575

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

This paper has been excerpted from the page proofs for the 2015 update to *E-Commerce and Internet Law: Treatise with Forms 2d Edition* (Thomson West 2015 Annual Update), a 4-volume legal treatise by Ian C. Ballon, published by Thomson Reuters West Publishing, 395 Hudson Street, New York, NY 10014, (212) 337-8443, www.ianballon.net.

GT GreenbergTraurig

Ian C. Ballon

Shareholder
Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
JD, LLM, CIPP

Ballon@gtlaw.com
Google+, LinkedIn, Twitter, Facebook: Ian Ballon

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

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

Ian Ballon represents Internet, technology, and entertainment companies in copyright, intellectual property and Internet litigation, including the defense of privacy and behavioral advertising class action suits. He is also the author of the leading treatise on Internet law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 4-volume set published by West (www.IanBallon.net). In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009) and serves as Executive Director of Stanford Law School's Center for E-Commerce.

Mr. Ballon, who practices in both Silicon Valley and LA, has brought or defended novel suits involving computer software, user generated content, rights in the cloud and in social media, links, frames, sponsored links, privacy and security, database protection, screen scraping and content aggregation, digital music, the Digital Millennium Copyright Act, rights of privacy and publicity, the enforceability of Internet Terms of Use and Privacy Policies and preemption under the CDA. A list of recent cases may be found at www.GTLaw.com/People/IanCBallon.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2013 edition of Best Lawyers in America. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award and named new media lawyer of the year in 2012 by the Century City Bar Association. He is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also has been recognized by *The Daily Journal* as one of the Top 75 IP litigators and Top 100 lawyers in California and is consistently listed as a top Northern California and Southern California litigator. Mr. Ballon also holds the CIPP certificate for the International Association of Privacy Professionals (IAPP).

27.07 Class Actions and Other Security Breach Litigation

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

Litigation 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

---

[Section 27.07]

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

[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).

confidential trade secrets were taken),[3] Copyright law[4] or various claims relating to database protection[5] (if material taken is copied), the Computer Fraud and Abuse Act[6] or common law trespass[7] (for an unauthorized intrusion), the Electronic Communications Privacy Act[8] (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.[9]

Where companies are sued by consumers or their business customers over a security breach, the most common theories of recovery are breach of contract, breach of implied contract, breach of fiduciary duty, public disclosure of private facts and negligence, depending on the facts of a given case. Security breach suits brought by consumers against companies that have experienced a breach therefore frequently are framed in terms of common law and state statutory remedies. Those few federal statutes that impose express data security obligations on persons and entities—The Children's Online Privacy Protection Act[10] (which regulates information collected from children under age 13), The Gramm-Leach-Bliley Act (which imposes security obligations on financial institutions[11]) and the Health Insurance Portability and Account-

---

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

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

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

[6]18 U.S.C.A. § 1030; *see generally infra* § 44.08.

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

[8]18 U.S.C.A. §§ 2510 to 2521 (Title I), 2701 to 2711 (Title II); *see generally infra* §§ 44.06, 44.07.

[9]*See infra* § 27.08[10].

[10]15 U.S.C.A. §§ 6501 to 6506; *supra* §§ 26.13[2], 27.04[2].

[11]15 U.S.C.A. §§ 6801 to 6809, 6821 to 6827; *supra* § 27.04[3].

ability Act (HIPAA)[12] (which regulates personal health information)—typically do not authorize a private cause of action (although the same underlying conduct that violates obligations under these laws potentially could be actionable under other theories of recovery). Claims also sometimes are asserted under federal computer crime statutes, such as the Stored Communications Act[13] but those statutes usually aren't well suited to data breach cases.[14] Claims arising out of security breaches also have been brought under the Fair Credit Reporting Act,[15] but that statute imposes obligations on consumer reporting agencies, users of consumer reports and furnishers of information to consumer reporting agencies,[16] and therefore does not provide a general remedy in the case of security breaches if the defendant is not a

---

[12]42 U.S.C.A. §§ 1320d *et seq.*; *supra* § 27.04[4].

[13]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).

[14]*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 information and PIN numbers from PIN pads in defendant's stores; holding that Michaels Stores was neither an ECS provider nor an RCS provider and therefore not subject to the SCA).

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

[15]15 U.S.C.A. §§ 1681 *et seq.*

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

member of one of those three groups.[17] Where a company fails to provide notice to consumers, it also potentially could be sued for statutory remedies in those states that afford a private cause of action to enforce rights under state security breach notification laws. Public companies that experience data breaches also may be subject to securities fraud class action suits.[18]

A company's obligation to comply with security breach notification laws often results in publicity that leads to litigation, including class action litigation, as well as regulatory scrutiny (which alternatively may lead to litigation).[19]

Higher stakes security breach litigation typically is brought by business customers of a company that has experienced a breach over which party bears the risk of loss. By contrast, consumers often are insulated from the financial consequences of a security breach.

In cases involving credit card theft, for example, credit card companies sometimes cancel accounts before consumers could be impacted (or refund the maximum $50 charge that a customer could incur as a result of credit card fraud under

---

[17]*See, e.g.*, *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 652–53 (S.D. Ohio 2014) (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); *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 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); *Burton v. MAPCO Express, Inc.*, __ F. Supp. 2d __, 2014 WL 4686479, at *6 (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.*, __ F. Supp. 2d __, 2014 WL 9608616, at *8 (N.D. Ill. 2014) (dismissing a FCRA claim where the defendant in a security breach case was not a "consumer reporting agency," which is defined as an entity engaged in the practice of assembling or evaluating consumer credit information for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing reports, 15 U.S.C.A. § 1681a(f), and could not allege that Trustwave's "purpose" was to furnish the information to data thieves).

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

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

federal law).[20] While potential plaintiffs may have a justified apprehension of potential future harm that could result from identity theft, that apprehension may not translate to present injury or damage sufficient to establish Article III standing or state a claim (or, where it is, it may not be directly traceable to a particular breach, or a particular company's responsibility for the breach, as opposed to other factors).

When a breach occurs, and an actual financial loss can be established, a plaintiff may maintain suit for breach of contract, breach of fiduciary duty, negligence or similar claims, depending on the facts of a given case.[21] These common law claims rarely afford either statutory damages or attorneys' fees and, as a consequence, in most consumer security breach cases standing to sue in federal court may present a real obstacle.

In most consumer cases there has been a violation but no immediate injury (and in many cases there never will be). In rare instances, a suit may be brought where emotional injuries can be shown,[22] but more often than not (as discussed later in this section) the economic loss doctrine

---

[20]*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).

[21]*See, e.g., 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).

[22]*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

bars recovery of damages for potential emotional injuries arising from fear and apprehension of potential identity theft.

As one court observed, under current pleading standards it 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."[23]

Standing must be established based on the named plaintiffs that actually filed suit, not unnamed putative class members.[24]

Most security breach suits where standing is an issue involve an actual security breach, but individual harm may be absent or merely *de minimis*. In such cases, plaintiffs' counsel frequently argue that plaintiffs have standing based on the risk of future harm, the costs associated with mitigating that risk (if any) and/or the loss of value experienced by

---

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.").

[23]*Burton v. MAPCO Express, Inc.*, __ F. Supp. 2d __, 2014 WL 4686479, at *1 (N.D. Ala. 2014).

[24]*See, e.g.*, *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976) ("That a suit may be a class action . . . adds nothing to the question of standing, for even named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.' "; quoting *Warth v. Seldin*, 422 U.S. 490, 502 (1975)); *see also O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) ("if none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class."); *Payton v. County of Kane*, 308 F.3d 673, 682 (7th Cir. 2002) ("Standing cannot be acquired through the back door of a class action." (internal quotation omitted)); *see also Easter v. American West Financial*, 381 F.3d 948, 962 (9th Cir. 2004) (holding that a court must first evaluate the standing of named plaintiffs before determining whether a class may be certified).

paying for a product or service that plaintiffs allege was over-priced based on the actual level of security provided.

Plaintiffs' counsel sometimes seek 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 is a present loss occasioned by the breach.[25] Some courts, however, have rejected the notion that credit monitoring costs can confer standing where the threat that these costs address is itself viewed as speculative or at least not certainly impending.[26] As the U.S. Supreme Court explained in *Clapper v. Amnesty International USA*,[27] plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[28] Although at the margins and in some courts plaintiffs' counsel may still be able to allege an injury suf-

---

[25]For this reason, companies that experience a security breach sometimes voluntarily offer affected consumers free credit monitoring services to deprive plaintiffs' counsel of a potential argument for standing to sue in litigation in federal court. *See generally infra* § 27.08 (analyzing state security breach notification laws and alternative responses, including offering credit monitoring services).

[26]*See, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012); *Remijas v. Neiman Marcus Group, LLC*, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014); *Moyer v. Michael's Stores, Inc.,* No. 14 C 561, 2014 WL 3511500, at *4 (N.D. Ill. July 14, 2014); *In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *7 (D.D.C. 2014); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 657–58 (S.D. Ohio 2014); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 470–71 (D.N.J. 2013). As one court explained:

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

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.*, __ F. Supp. 2d __, 2014 WL 4379916, at *9-10 (N.D. Cal. 2014) (holding that where the court found that plaintiffs adequately alleged that they faced "a certainly impeding future harm from the theft of their personal data, . . . the costs Plaintiffs . . . incurred to mitigate this future harm constitute an additional injury–in–fact.").

[27]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013).

[28]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1143, 1151 (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 confidential-

ficient to meet standing requirements, in general it is getting more difficult for plaintiffs to establish standing to sue in security breach cases absent real injury, even as the volume of security breaches continues to skyrocket.

Prior to *Clapper*, the Seventh[29] and Ninth[30] Circuits and district courts elsewhere[31] held that consumers impacted by

---

ity 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.*

[29]*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.

[30]*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 Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908 (N.D. Cal. 2009) (holding, prior to *Krottner,* that a job applicant whose personal information (including his Social Security number) had been stored on a laptop of the defendant's that had been stolen had standing to sue but granting summary judgment for the defendant where the risk of future identity theft did not support claims for negligence, breach of contract, unfair competition or invasion of privacy under the California constitution), *aff'd mem.,* 380 F. App'x 689 (9th Cir. 2010). *But see In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (dismissing plaintiffs' putative class action suit arising out of a hacker gaining access to their LinkedIn passwords and email addresses, for lack of Article III standing, where plaintiffs alleged no injury or damage).

[31]*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,*

security breaches where data has been accessed by unauthorized third parties, but no loss has yet occurred, have standing[32] 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[33] (and various district courts in other circuits[34] have found the threat of future

---

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).

[32]To have standing to bring suit in federal court, a plaintiff must have suffered an "injury in fact," which must be (a) "concrete and particularized" and (b) "actual or imminent, not conjectural or hypothetical." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). More specifically, "[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.' " *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (2013), *quoting Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149-50 (2010); *see generally supra* § 26.15 (analyzing standing in greater depth in connection with data privacy class action cases).

[33]*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,* 132 S. Ct. 2395 (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).

[34]*See, e.g., 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.");

harm to be too speculative to support standing).

In *Reilly v. Ceridian Corp.*,[35] 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

---

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

[35]*Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied,* 132 S. Ct. 2395 (2012).

quantify how it will manifest itself."[36] In data breach cases where no misuse is alleged, however, "there has been no injury—indeed, no change in the status quo . . . . [T]here is no quantifiable risk of damage in the future . . . . Any damages that may occur . . . are entirely speculative and dependent on the skill and intent of the hacker."[37]

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."[38] Similarly, standing in environmental injury cases is unique "because monetary compensation may not adequately return plaintiffs to their original position."[39] 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."[40]

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."[41]

While there is 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 evi-

---

[36]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 132 S. Ct. 2395 (2012).

[37]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 132 S. Ct. 2395 (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.*

[38]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 132 S. Ct. 2395 (2012).

[39]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011), *cert. denied,* 132 S. Ct. 2395 (2012).

[40]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 45–46 (3d Cir. 2011) (emphasis in original), *cert. denied,* 132 S. Ct. 2395 (2012).

[41]*Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011), *cert. denied,* 132 S. Ct. 2395 (2012).

dence of present injury, is weak. In *Katz v. Pershing, LLC,*[42] the First Circuit distinguished both the Third Circuit's holding in *Ceridian*[43] and Seventh and Ninth Circuit opinions finding standing in data breach suits,[44] 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 support Article III standing.[45]

In *Frezza v. Google Inc.*,[46] 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*

---

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

[43]*Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied,* 132 S. Ct. 2395 (2012).

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

[45]*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).

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

International USA,[47] emphasized that to establish standing "allegations of possible future injury are not sufficient."[48] The threatened injury must be "certainly impending" to constitute injury in fact.[49] 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] 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.[51]

Clapper arguably makes it even more difficult for plaintiffs in security breach cases to establish standing in the absence of identity theft. Indeed, courts in many data security cases have read *Clapper* this way,[52] although at least two cases in California have distinguished *Clapper* and found that secu-

---

[47]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013).

[48]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (2013) (internal quotation marks omitted).

[49]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1146–47 (2013).

[50]50 U.S.C.A. § 1881a.

[51]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1148 (2013).

[52]*See, e.g., Remijas v. Neiman Marcus Group, LLC*, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014) (dismissing claims arising out a security breach involving the potential disclosure of payment card data and personally identifiable information from 350,000 customers because (1) the alleged increased risk of future harm was insufficient to establish standing where plaintiffs alleged that their data *may* have been stolen and that 9,200 people, or approximately 2.5% of the affected group of customers, had fraudulent charges appear on their credit cards, (2) the time and money spent to mitigate the risk of future fraud and identity theft was insufficient absent unreimbursed charges or other allegations of some substantial attendant hardship and (3) plaintiffs failed to allege more than *de minimis* injury and standing could not be based on plaintiffs allegedly having paid a premium for the retail goods purchased at defendant's stores where the value-reducing deficiency was not intrinsic to the product itself); *Burton v. MAPCO Express, Inc.*, __ F. Supp. 2d __, 2014 WL 4686479, at *1–5 (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.*, __ F. Supp. 2d __, 2014 WL 1858458 (D.D.C. 2014) (dismissing claims brought on behalf of 4.7 million

rity breach plaintiffs had standing to assert claims based on increased risk of harm under pre-*Clapper* Ninth Circuit law.[53]

---

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); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014) (holding that (1) the alleged increased risk that consumers would be victims of identity theft at some indeterminate time in the future (alleged by plaintiffs to be 9.5 times more likely than members of the general public, reflecting a fraud incidence rate of 19%), and expenditures to mitigate that potential future risk was not "certainly impending" and therefore did not constitute injury sufficient to confer standing, and (2) consumers' allegation that they suffered a loss of privacy when their personally identifiable information was stolen did not constitute injury sufficient to confer standing to bring negligence or bailment claims, although it did establish standing to sue for state law invasion of privacy); *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 4759855 (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).

[53]*See In re Adobe Systems, Inc. Privacy Litig.*, __ F. Supp. 2d __, 2014 WL 4379916 (N.D. Cal. 2014) (holding that plaintiffs had standing to assert claims under Cal. Civil Code § 1798.81.5 and for declaratory relief for failing to maintain allegedly reasonable security and for unfair competition for failing to warn about allegedly inadequate security in a case involving a security breach exposing the user names, passwords, credit and debit card numbers, expiration dates, and email addresses of 38 million customers; dismissing plaintiffs' claim for alleged delay in providing consumer notice, where there was no traceable harm, and plaintiffs' claim that they had spent more for Adobe products than they would have had they known the true level of security); *In re Sony Gaming Networks & Customer Data Security Breach Litig.*, 996 F. Supp. 2d 942, 960-63 (S.D. Cal. 2014) (holding that plaintiffs had standing to sue based on allegations that their personal information was collected by Sony and then wrongfully disclosed as a result of a security breach, where the court concluded that *Clapper* was not inconsistent with *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010)).

In *Adobe*, Judge Lucy 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. She also distinguished *Clapper* because that case *Clapper*'s discussion of 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." *Id.*, *citing Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (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 and internal quotation marks omitted). Judge Koh 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 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.

In re Adobe Systems, Inc. Privacy Litig., __ F. Supp. 2d __, 2014 WL 4379916, at *8 (N.D. Cal. 2014). In the alternative, she ruled that even if *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010) was "no longer good law, the threatened harm alleged . . . [in *Adobe* was] sufficiently concrete and imminent to satisfy *Clapper*." 2014 WL 4379916, at *8. 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," 133 S. Ct. at 1148, 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, *see* 133 S. Ct. at 1148, . . . [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

District courts in the Seventh Circuit also have disagreed over whether *Clapper* tightened the standards for establishing standing based on the elevated risk of identity theft stemming from a data breach or whether *Pisciotta v. Old National Bancorp*.[54] was still controlling even after *Clapper*.[55]

---

will be able to do so." *Id.* In so ruling, Judge Koh distinguished *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 456 (D.N.J. 2013), 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.*, __ F. Supp. 2d __, 2014 WL 960816, at *6–7 (N.D. Ill. 2014) and *In re Barnes & Noble Pin Pad Litig.,* No. 12 C 8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013), as cases where it was not clear that any data had been stolen at all.

By contrast, Judge Koh disagreed with *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014), 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." 2014 WL 4379916, at *9. 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? . . . ." *Id.* at *9. Regardless, she wrote, *Galaria*'s reasoning lacked force in *Adobe,* where plaintiffs allegedthat some of the stolen data already had been misused. *Id.*

In a footnote, Judge Koh noted further 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 traceable' to the defendant's data breach." 2014 WL 4379916, at *8 n.5.

In *Sony Gaming,* the court reiterated its earlier ruling, decided before *Clapper*, that the plaintiffs had standing to sue under *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010). 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.' " *In re Sony Gaming Networks & Customer Data Security Breach Litig.*, 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014).

[54]*Pisciotta v. Old National Bancorp.*, 499 F.3d 629 (7th Cir. 2007).

[55]*Compare, e.g., Strautins v. Trustware Holdings, Inc.*, __ F. Supp. 2d __, 2014 WL 960816, at *4 (N.D. Ill. 2014) (Tharp, J.) ("*Clapper* compels rejection of Strautins' claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing."); *In re Barnes & Noble Pin Pad Litig.,* No. 12 C 8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) (Darrah, J.) (citing *Clapper* in support of the proposition

As an example of the more typical analysis undertaken since *Clapper,* in *In re SAIC Corp.*,[56] the U.S. District Court for the District of Columbia held that the risk of identity theft alone and invasion of privacy to be insufficient to constitute "injury in fact," and the allegation that plaintiffs lost personal medical information to be too speculative in a security breach involving 4.7 million members of the U.S. military and their families. The court held that mere allegations that unauthorized charges were made to plaintiffs' credit and debit cards following the theft of data failed to show causation, but allegations that a specific plaintiff received letters in the mail from a credit card company thanking him for applying for a loan were sufficient. Similarly, the court held that the allegation that a plaintiff received a number of unsolicited calls from telemarketers and scam artists following the data breach did not suffice to show causation, but the allegation that unsolicited telephone calls were received on a plaintiff's unlisted number from insurance companies and others targeted at her specific, undisclosed medical condition were sufficient.[57]

In so ruling, Judge James E. Boasbert, 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."[58] 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 . . . .

---

that "[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing"); *with Moyer v. Michael's Stores, Inc.,* No. 14 C 561, 2014 WL 3511500, at *4–6 (N.D. Ill. July 14, 2014) (Bucklo, J.) (holding that the plaintiffs in a security breach class action suit had standing to sue based on the elevated risk of identity theft stemming from a data breach under *Pisciotta* and explaining *Clapper* as a case that applied the imminence requirement for standing in an "especially rigorous" fashion because of the national security and constitutional issues raised by that case, which sought to hold the Foreign Intelligence Surveillance Act Amendments Act of 2008 unconstitutional).

[56]*In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458 (D.D.C. 2014).

[57]*In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458 (D.D.C. 2014).

[58]*In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *6 (D.D.C. 2014).

> 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.[59]

Judge Boasbert 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 information could be in danger."[60] 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."[61]

Judge Boasbert 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

---

[59] *In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458 (D.D.C. 2014).

[60] *In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *7 (D.D.C. 2014).

[61] *In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *7 (D.D.C. 2014), *quoting Clapper*, 133 S. Ct. at 1147–48.

avoid the harm.'"[62] 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.").[63]

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."[64] 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 Boasbert 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 "certainly impending."[65] 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

---

[62] *In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *7 (D.D.C. 2014), *quoting Clapper,* 133 S. Ct. at 1150 n.5 (emphasis added by Judge Boasbert).

[63] *In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *7 (D.D.C. 2014).

[64] *In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *13 (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.").

[65] *Clapper*, 133 S. Ct. at 1147.

> 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.[66]

In a small percentage of cases, security breach claims may be brought under federal statutes.[67] If so, courts in some circuits will find standing where a plaintiff can state all of the elements of a claim for relief under a federal statute, even if the plaintiff cannot show any demonstrable injury or harm. In other circuits, however, even this more relaxed approach to standing under federal statutes will not hold.

Courts in the Sixth, Eighth and Ninth Circuits will find standing where a plaintiff can state a claim for violation of a statute that does not require a showing of actual harm.[68] Courts in the Ninth Circuit have construed this rule, first articulated in *Edwards v. First American Corp.*,[69] 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

---

[66]*In re SAIC Corp.*, ___ F. Supp. 2d ___, 2014 WL 1858458, at *13–14 (D.D.C. 2014).

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

[68]*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 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); *Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), *cert. dismissed,* 132 S. Ct. 2536 (2012); *supra* § 26.15.

[69]*Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), *cert. dismissed,* 132 S. Ct. 2536 (2012).

is particularized as to them."[70]

The Fourth and Federal Circuits, however, do not accept the proposition that alleging an injury-in-law by stating a claim and establishing statutory standing to sue satisfies the constitutional standing requirements of Article III.[71]

Most consumer security breach putative class action suits, however, as previously noted, are brought under contract, quasi-contract or other state law theories of recovery. Accordingly, relaxed standards for standing in federal question cases will not apply in many cases. Even where standing is established, security breach claims based on potential future harm have proven difficult to maintain in the absence of any injury in either state[72] or federal appellate[73] and district[74] courts. While a company may have a contractual claim

---

[70]*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.

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

[72]*See, e.g., Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 708–11 (D.C. 2009) (dismissing claims by participants against a plan administrator for negligence, gross negligence and breach of fiduciary duty because participants did not suffer any actual harm as a result of the theft of a laptop computer, and for invasion of privacy because plaintiff's allegation that defendants failed to implement adequate safeguards did not support a claim for intentional misconduct); *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 455 Mass. 458, 918 N.E.2d 36 (Mass. 2009) (affirming dismissal of contract and negligence claims and summary judgment on the remaining of the issuing credit unions' claims against a retailer that had improperly stored data from individual credit cards in a manner that allowed thieves to access the data, and against the retailer's acquiring bank that processed the credit card transactions, where the credit unions were not third-party beneficiaries to the agreements between the retailer and acquiring bank, plaintiffs' negligence claims were

against a third party vendor responsible for a security

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).

[73]*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

breach, consumer contracts rarely provide such assurances

---

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); *Stollenwerk v. Tri–West Health Care Alliance*, 254 F. App'x 664, 666–68 (9th Cir. 2007) (affirming summary judgment on claims for damages for credit monitoring services under Arizona law entered against two plaintiffs whose names, addresses and Social Security numbers were stored on defendant's stolen computer servers but who "produced evidence of neither significant exposure of their information nor a significantly increased risk that they will be harmed by its misuse" and reversing summary judgment granted against a third plaintiff who had presented evidence showing a causal relationship between the theft of data and instances of identity theft).

[74]*See, e.g.*, *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 re Sony Gaming Networks and 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 and Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942 (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 Com-

munications Act claim; dismissing plaintiffs' Illinois Consumer Fraud and Deceptive Business Practices Act claim based on deceptive practices because plaintiffs could not identify a specific communication that allegedly failed to disclose that the defendant had allegedly failed to implement adequate security measures, but allowing the claim to the extent based on unfair practices in allegedly failing to comply with Visa's Global Mandate and PCI Security requirements and actual losses in the form of unauthorized bank account withdrawals, not merely an increased risk of future identity theft and costs of credit monitoring services, which do not satisfy the injury requirement; and denying plaintiffs' motion to dismiss claims under the Illinois Personal Information Protection Act (based on the alleged failure to provide timely notice of the security breach) and for breach of implied contract); *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.,* M.D.L. No. 09-2146, Civil Action No. H-10-171, 2011 WL 1232352 (S.D. Tex. Mar. 31, 2011) (dismissing with prejudice financial institution plaintiffs' claims against credit card processor defendants for negligence, based on the economic loss doctrine, and dismissing without prejudice claims for breach of contract (alleging third party beneficiary status), breach of fiduciary duty and vicarious liability); *Hammond v. Bank of N.Y. Mellon Corp.,* No. 08–6060, 2010 WL 2643307, at *4, *7 (S.D.N.Y. June 25, 2010) (finding no standing and, in the alternative, granting summary judgment on plaintiff's claims for negligence, breach of fiduciary duty, implied contract (based on the absence of any direct relationship between the individuals whose data was released and the defendant) and state consumer protection violations based on, among other things, the absence of any injury, in a case where a company owned by the defendant allegedly lost computer backup tapes that contained the payment card data of 12.5 million people); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908 (N.D. Cal. 2009) (holding that a job applicant whose personal information had been stored on a laptop of the defendant's that had been stolen had standing to sue but granting summary judgment for the defendant where the risk of future identity theft did not rise to the level of harm necessary to support plaintiff's negligence claim, which under California law must be appreciable, non-speculative, and present; breach of contract claim, which requires a showing of appreciable and actual harm; unfair competition claim, where an actual loss of money or property must be shown; or claim for invasion of privacy under the California constitution, which may not be premised on the mere risk of an invasion or accidental or negligent conduct by a defendant), *aff'd mem.,* 380 F. App'x 689 (9th Cir. 2010); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605 (S.D.N.Y. 2009) (dismissing plaintiff's negligent misrepresentation claim under the economic loss doctrine and dismissing claims for violations of N.Y. Gen. Bus. L. § 349, breach of fiduciary duty and breach of contract for the alleged disclosure of plaintiff's email address and the potential dissemination of certain personal information from his bank account with the defendant bank for failure to plead actual injury or damages because "the release of potentially sensitive information alone, without evidence of misuse, is insufficient to cause damage to a plaintiff . . . , the risk of some undefined future harm is too speculative to constitute a compensable injury" and the receipt of spam by itself does not constitute a sufficient injury); *Pinero v. Jackson Hewitt Tax Service Inc.*, 594

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

and individuals usually are not intended beneficiaries of corporate security contracts with outside vendors.[75] Negligence claims likewise typically fail based on the economic loss doctrine, which holds that purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage. Breach of fiduciary duty claims also often fail in the absence of a fiduciary obligation. Breach of contract, breach of implied contract and unfair competition claims likewise may fail where there has been no economic loss. Claims based on delay in providing notification also may fail in the absence of any actual injury proximately caused by the alleged delay.[76]

State security statutes also may provide defenses. For example, in *In re Sony Gaming Networks and Customer Data Security Breach Litigation*,[77] 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

---

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).

[75]*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).

[76]*See, e.g., In re Adobe Systems, Inc. Privacy Litig.*, __ F. Supp. 2d __, 2014 WL 4379916 (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 4759855 (N.D. Ill. Sept. 3, 2013) (rejecting the argument that the delay or inadequacy of breach notification increased plaintiffs' risk of injury).

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

1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively."[78] The court reasoned that claims by California resident 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, none of Plaintiffs current allegations assert willful, intentional, or reckless conduct on behalf of Sony."[79]

In *Sony,* among other rulings, the court also dismissed plaintiffs' claim for bailment, holding that personal information could not be construed as property that was somehow "delivered" to Sony and expected to be returned, and because the information was stolen as a result of a criminal intrusion of Sony's Network.[80]

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 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

---

[78]*In re Sony Gaming Networks and 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).

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

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

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 § 1789.84(e) (but not damages under section 1789.84(b)) and partial performance and breach of the implied duty of good faith and fair dealing,[81] even as the court dismissed multiple other claims for negligence, negligent misrepresentation/omission, unjust enrichment and state consumer protection laws.

Where a security breach has led to identity theft, unauthorized charges or other injury, a plaintiff will be more likely to be able to state a claim.[82] For example, in *Anderson*

---

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

[82] *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

v. Hannaford Brothers Co.,[83] 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

---

numbers had been stored on defendant's stolen computer servers); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (holding that victims of identity theft had stated claims for negligence, breach of fiduciary duty, breach of contract, breach of implied contract, and unjust enrichment/restitution, in a suit arising out of the disclosure of sensitive information of 1.2 million current and former AvMed members (including protected health information, Social Security numbers, names, addresses and phone numbers) when two laptops containing unencrypted data were stolen from the 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).

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

information."[84] The court explained that:

> When a customer uses a credit card in a commercial transaction, 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.[85]

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.[86] 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."[87] Unlike cases based on inadvertently misplaced or loss 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."[88] The court noted that the fact that many banks and credit card issuers immediately

---

[84]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 159 (1st Cir. 2011).

[85]*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).

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

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

[88]*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

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.[89]

On the other hand, the appellate panel agreed with the district court that non-mitigation costs—such as fees for pre-authorization 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.[90]

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

---

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 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).

[89]*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.

Anderson v. Hannaford Brothers Co., 659 F.3d 151, 164–65 (1st Cir. 2011).

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

maintain reasonable security.[91] The court's holding, however, turned on the narrow nature of Maine's unfair competition 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.[92]

On remand, the lower court denied plaintiffs' motion for class certification, finding that common questions of law and fact did not predominate.[93]

In *Resnick v. AvMed, Inc.,*[94] 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 v. AvMed,* ten months after the laptop theft, identity thieves opened Bank of America accounts in the name of one of the plaintiffs, activated and used credit cards for unauthorized purchases and sent a change of address notice to the U.S. postal service to delay plaintiff learning of the unauthorized accounts and charges. Fourteen months after the theft 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

---

[91]*Anderson v. Hannaford Brothers Co.*, 659 F.3d 151, 159 (1st Cir. 2011).

[92]*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).

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

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

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."[95]

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.[96] In *Resnick v. AvMed, Inc.*, 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.[97]

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*,[98] 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 businesses and their financial institutions.[99] *Patco* was a suit brought over six fraudulent withdrawals, totaling

---

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

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

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

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

[99]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."

$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[100] (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 . . . ."[101]

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 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

---

Patco Construction Co. v. People's United Bank, 684 F.3d 197, 207 n.7 (1st Cir. 2012).

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

[101]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).

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.[102]

By contrast, in *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*,[103] 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. Choice had declined to place dollar limits on daily transactions or use dual control. In November 2009, Choice 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

---

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

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

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."[104] For example, in *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.*,[105] the court dismissed the financial institution plaintiffs' claims for fraud and misrepresentation against a credit and debit card processor whose computer systems had been compromised by hackers, with leave to amend to allege factually concrete and verifiable statements, rather than mere puffery, made prior to, rather than after the security breach, to the extent relied 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 reason-

---

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

[105]*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).

ably rely.[106] 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."[107]

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.[108]

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

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

---

[106] *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).

[107] *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).

[108] *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).

verification process validating compliance with VISA requirements for data security"[109]

Despite the prevalence of security breaches, the volume of security breach class action litigation has not been as large as one might expect. Indeed, despite the potential for more substantial economic harm when a security breach occurs, there has not been an explosion of security breach class action suits to rival the large number of data privacy suits filed since 2010 over the alleged sharing of information with Internet advertisers and online behavioral advertising practices.[110] There may be several explanations for this. First, when a security breach occurs, cases brought by consumers often settle if there genuinely has been a loss (even if litigation with insurers and third parties over liability may continue). In consumer cases, the amount of individual losses may be limited both because security breaches do not always result in actual financial harm and because, when they do, federal law typically limits an individual consumer's risk of loss to $50 in the case of credit card fraud (and many credit card issuers often reimburse even that amount so that customers in fact incur no direct out of pocket costs). Class action settlements therefore may be focused on injunctive relief and *cy pres* awards, rather than large damage sums.[111]

Second, since security breaches often revolve around a

---

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

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

Id. at 593.

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

[111]*See, e.g.*, *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*

common event, multiple cases may be more likely to be consolidated by the Multi-District Litigation (MDL) panel.[112] By contrast, behavioral advertising privacy cases may involve similar alleged practices engaged in by multiple, unrelated companies or even entire industries, in somewhat different ways. Similar data privacy cases therefore typically have been brought as separate putative class action suits against different companies (or a single technology company and some of its customers). A particular alleged practice therefore may spawn dozens of analogous lawsuits against different companies that do not end up being consolidated by the MDL Panel.

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

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

Some courts also have been more receptive to claims in security breach cases where real losses were experienced. For example, in *Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*,[113] 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,

---

pres payments totaling $998,075 to third party organizations and $606,192.50 in attorneys' fees).

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

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

such as the Issuer Banks, constituted an "identifiable class," the defendant (in this case, Heartland) had reason to foresee that members of the identified class would be the entities to suffer economic losses were the defendant negligent, and the defendant would not be exposed to "boundless liability," but rather to the reasonable amount of loss from a limited number of entities; and (2) in the absence of a tort remedy, the plaintiffs, like the Issuer Banks in Heartland, would be left with no remedy at all for negligence, defying "notions of fairness, common sense and morality."

Contract limitations, while beneficial to companies in security breach litigation, may be more difficult to enforce against consumers. Marketing considerations may limit a company's ability to disclaim security obligations. Moreover, as a practical matter, it is unclear whether security obligations could ever be fully disclaimed in a consumer contract. The Federal Trade Commission has taken the position that a company's failure to maintain adequate security, even in the absence of affirmative representations, is an actionable violation of unfairness prong of section 5 of the Federal Trade Commission Act.[114] The FTC or state Attorneys' General could bring enforcement actions or otherwise seek to apply pressure on a company that purported to disclaim obligations. Some security law obligations likewise may not be waived.

Since FTC Act violations are potentially actionable as violations of state unfair competition laws in some jurisdictions, a company's failure to adhere to implement reasonable security measures could be separately actionable regardless of what a company says about its practices. For example, California's notorious unfair competition statute, Cal. Bus. & Prof. Code § 17200, allows a private cause of action to be brought for violations of other statutes that do not expressly create independent causes of action[115] (although only provided that the plaintiff has "suffered injury in fact and has lost money or property";[116] as a result of the violation).

While security breach class action suits may not have been

---

[114]*See supra* § 27.06.

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

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

as lucrative for plaintiffs' counsel as some might imagine—and even where a claim can be asserted a class may not be certified[117]—major security breaches have cost companies and their insurers substantial money.[118]

As security law and practice evolves, the risks of litigation increase. FTC enforcement actions have encouraged the development of security-related best practices, including the adoption of information security programs. In addition, particular statutes, such as the Massachusetts law affirmatively mandating information security programs,[119] compel particular practices. Security breach notification statutes have created an even stronger incentive for businesses to address security concerns. Indeed, the requirement that companies notify consumers and in some cases state regulators of security breaches creates a tangible risk of litigation and regulatory enforcement actions—without any safe harbor to insulate businesses in the event a breach occurs despite best efforts to prevent one. Many of these statutes afford independent causes of action. Other state laws, such as California Bus. & Prof. Code § 1798.81.5—which compels businesses that own or license personal information about California residents to implement and maintain *reasonable* security procedures and practices appropriate to the nature of the information, to protect it from unauthorized access, destruction, use, modification or disclosure—cannot be disclaimed and further invite potential litigation in the absence of any express definition of, or safe harbor for, what might be deemed *reasonable*. Significantly, courts evaluating state law claims are not necessarily bound by the principle recognized by the FTC that "security breaches sometimes can happen when a company has taken every reasonable precaution."[120]

Without specific guidelines—such as those applied to financial institutions and covered health care entities under federal law—what constitutes adequate or reasonable conduct ultimately may present a fact question in litigation.

---

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

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

[119]*See supra* § 27.04[6][E].

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

The absence of safe harbors for businesses outside of the health care and financial services industries means that even businesses that implement the latest security technologies and industry "best practices" may be forced to defend themselves in litigation if a security breach occurs. As the cases discussed in this section illustrate, whether a claim for a breach is viable may depend on whether consumers are injured, which companies cannot easily control, and whether risk of loss provisions are addressed in contracts with vendors, banks, insurers and others, which a company may be able to influence, depending on its negotiating position and diligence in auditing its security-related agreements.

A company may limit its risk of litigation by entering into contracts with binding arbitration provisions and class action waivers, at least to the extent that there is privity of contract with the plaintiffs in any putative class action suit. While class action waivers are not universally enforceable, a class action waiver that is part of a binding arbitration agreement is enforceable as a result of the U.S. Supreme Court's 2011 decision in *AT&T Mobility LLC v. Concepcion*.[121]

Even without a class action waiver, certification of a privacy or security-related class action may be difficult to obtain where users enter into agreements that provide for binding arbitration of disputes.[122] Arbitration provisions are broadly enforceable and, if structured properly, should insulate a company from class action litigation brought by any person with whom there is privity of contract.[123]

Where a claim is premised on an interactive computer service provider's republication of information, rather than direct action by the defendant itself, claims against the

---

[121]*AT&T Mobility LLC v. Concepcion*, 131 S. Ct. 1740 (2011); *see generally supra* § 22.05[2][M] (analyzing the decision and more recent cases construing it and providing drafting tips for preparing a strong and enforceable arbitration provision); *see also supra* § 21.03 (online contract formation).

[122]*See, e.g., 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).

[123]*See supra* § 22.05[2][M][i] (analyzing *AT&T Mobility LLC v. Concepcion*, 131 S. Ct. 1740 (2011) and ways to maximize the enforceability of arbitration provisions).

provider may be preempted by the Communications Decency Act.[124]

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

[124]47 U.S.C.A. § 230(c); *supra* § 37.05.

[Section 27.08[1]]

[1]A compendium of the security breach notification statutes and implementing regulations in effect in each state and territory as of August 1, 2014 is set forth in section 27.09. Those states that had not enacted security breach notification statutes as of that date were: **Alabama, New Mexico** and **South Dakota**. The analysis set forth in this section is based on notification statutes in force as of August 1, 2014.

[2]*See supra* § 27.04[3][C].

[3]*See supra* § 27.04[4].

[4]U.S. Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic 2—Cybersecurity (Oct. 13, 2011).

[5]*See supra* § 27.04[5][B].

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS,2D 2015

Ian C. Ballon

The most comprehensive authority available on digital media, the cloud, mobile, social media Internet and e-commerce law

THOMSON REUTERS™

TAKE YOUR INTERNET AND MOBILE PRACTICE TO THE NEXT LEVEL

E-Commerce & Internet Law is a comprehensive, authoritative work covering business-to-business and business-to-customer issues, regulatory issues, and emerging trends. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to more than 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 four sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Privacy, Security 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
- Liability of Internet and Mobile Sites and Services (Including Social Networks and Blogs)
- Civil Jurisdiction and Litigation

Questions to Answer as Internet law moves to mobile devices, social media and the cloud:

- Does content syndication to mobile providers take a service provider outside the DMCA?
- How does text marketing differ from email marketing?
- Privacy issues when dealing with users who are subject to COPPA or teenagers not subject to COPPA but subject to heightened concern
- Facebook and Twitter contacts as the basis for personal jurisdiction
- How to obtain substitute service over a foreign defendant in an Internet dispute

Key Features of E-Commerce & Internet Law

- The only treatise to comprehensively and exhaustively cover the liability of Internet and mobile service providers, cloud storage providers, bloggers, and owners and operators of social networks and other Web 2.0 applications
- Substantial caselaw coverage on Terms of Use and Internet contracts to help you draft better agreements, with sample forms and provisions
- Latest caselaw and analysis on sponsored links, key word sales, and liability for search engine optimization practices
- Includes coverage on enforcing judgments against domain names and the extent to which even unrelated claims against foreign defendants could be satisfied in U.S. courts
- Rethinking consumer criticism, gripe site, blog, and fan site law in light of new Lanham Act and CDA caselaw (including a checklist for evaluating potential claims and their viability)
- Comprehensive analysis of state law security breach notification statutes, together with practical tips on how to prepare for and respond to security breaches
- Extensive data on the prices paid for domain names and how to value them
- How to draft Privacy Policies, Terms of Use, and other documents and conduct website and privacy audits
- Practical tips, checklists, forms, and helpful information that goes well beyond what is usually included in a legal treatise
- Glossary terms drawn from the latest caselaw (helpful for briefs and contract definitions)
- Practical strategies for effectively documenting Internet transactions, drafting forms, and devising winning litigation strategies
- Exhaustive DMCA guidelines, CDA analysis, and strategies for managing user content
- Most thorough and clear cut analysis of Internet jurisdiction available anywhere
- Clear, concise, comprehensive and practical analysis

SUMMARY OF CONTENTS

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

NEW IN THE 2015 EDITION

****
ABOUT THE AUTHOR
****

IAN C. BALLON

Mr. Ballon, who is admitted to practice in California, the District of Columbia and Maryland and in the U.S. District Court for the District of Colorado, represents companies in copyright, trademark, trade secret, right of publicity, privacy and security and other Internet-related cases and in defense of data privacy, security, TCPA, advertising and Internet and mobile class action suits.

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 Daily Journal as one of the Top 75 Intellectual Property litigators and Top 100 lawyers in California.

Mr. Ballon is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also was recognized by the Los Angeles and San Francisco Daily Journal in 2009 for obtaining the third largest plaintiff's verdict in California in 2008 in MySpace, Inc. v. Wallace, which was one of several cases in which he served as lead counsel that created important precedents on the applicability of the CAN-SPAM Act, California's anti-phishing statute and other laws to social networks.

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. certification from the International Association of Privacy Professionals.

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

He may be contacted at ballon@gtlaw.com and followed on Google+, Twitter and LinkedIn (@IanBallon).

Contributing authors: Ed Chansky, Emilio Varanini , Tucker McCrady, Parry Aftab and Josh Raskin

- Exhaustive coverage of the latest law and trends in data privacy, data security, TCPA and CAN-SPAM Act litigation (including class action litigation) – the most comprehensive available anywhere!
- The U.S. Supreme Court's decision in *Aereo* and its impact on public performance and direct liability case law (and the continuing validity of *Cartoon Network* in light of *Aereo*)
- New standards for false advertising law based on the U.S. Supreme Court's 2014 opinions
- Patent law in light of *Alice* and other new U.S. Supreme Court opinions (updated by Joshua Raskin)
- Exhaustive circuit-by-circuit, claim-by-claim and fact pattern analysis of the CDA, 47 U.S.C. § 203(c) – the most comprehensive available anywhere!
- Understanding the TCPA, how it differs from the CAN-SPAM Act and whether and to what extent FCC rules and guidelines impact laws and litigation governing text marketing.
- The interplay between the DMCA, the CDA and other safe harbors, defenses and exemptions available to cloud service providers, operators of social networks, mobile providers, app developers and app store hosts, service providers and employer-owned computer networks.
- The parameters of federal preemption of right of publicity and other IP claims under the Telecommunications Act.
- The latest analysis on the interplay between Internet, cloud and mobile business and antitrust law (updated by Emilio Varanini)
- New sections addressing the common law copyright issues for sound recordings in digital media and California's law prohibiting sites and services from restricting user criticism
- Updated analysis of state security breach laws in the 48 states that have them and in D.C., Puerto Rico and Guam – analyzed holistically the way a practitioner would, rather than merely by chart or graph.
- Music licensing (updated by Tucker McCrady)
- Latest law and practice on how to draft, enforce and litigate Terms of Use agreements and privacy policies for websites and mobile devices
- Complete analysis of security breach case law, statutes and trends
- Mobile, Internet and social media contests and promotions (updated by Ed Chansky)
- Latest law on sponsored links, database protection, screen scraping and search engine optimization
- Complete, updated catalogue of state statutes governing state security breach notification laws, email marketing and online dating
- Latest case law on subpoenaing data from internet, mobile and social network sites and what is permissible under ECPA and state statutory and common law privacy laws
- Hundreds of new and recent cases and FTC data privacy, security and COPPA enforcement actions and settlements
- The most comprehensive authority available on the law of digital media, the cloud, mobile and social media law as well as e-Commerce and internet law.