FIFTY SHADES OF CLAIMS:
WHEN PRIVATE INFORMATION BECOMES PUBLIC IN THE UNITED STATES

Brad Jones, Partner, Meagher & Geer

I. INTRODUCTION

Every week ushers in a new data breach that makes national headlines. Last week, a hacker released private photos of celebrities such as Jennifer Lawrence, Kate Upton, and Ariana Grande.[30] And Home Depot is investigating a potential data breach possibly involving the credit and debit cards of customers at all of its stores.[31] Data breaches and cyber risk are nothing new. Although data breaches frequently occur, what is new are the escalating costs associated with experiencing and responding to a data breach. The cost to companies experiencing data breaches has steadily increased. The average data breach costs $201 per record, totaling $5.9 million, up 8% from the previous year.[32] In addition, companies experiencing data breaches must navigate a complex maze of requirements and potential liability under federal statutes and rules, state statutes, and state common law.

Courts addressing plaintiffs' claims in data-breach litigation have frequently found that plaintiffs lack standing to assert their claims or fail to state a claim upon which relief may be granted. But results in data-breach litigation depend in part on the jurisdiction and applicable law. Plaintiff lawyers will continue to search for new and creative ways to assert claims arising out of data breaches, and insurers involved with such litigation should remain aware of any developments in the law.

II. SOURCES OF LAW

A. Protected information

Regulation of personal information in the United States is multi-layered due to federal and state statutes and regulations, self-regulation (*e.g.*, Payment Card Industry Data Security Standard adopted by organizations handling cardholder information), and state common law. There is no single federal law providing a uniform classification of the types of personal information; information is classified by sector. For instance, the Health Insurance Portability and Accountability Act (HIPAA) concerns "protected health information" and "individually

[30] *See* Elizabeth Durand Streisand, *Jennifer Lawrence, Kate Upton and Many Other Female Stars Have Been Hacked*, https://celebrity.yahoo.com/blogs/celeb-news/jennifer-lawrence-and-many-other-female-stars-have-been-hacked-005149625.html.
[31] *See* Shelly Banjo, *Home Depot CEO: Probe Continues into Possible Data Breach*. http://online.wsj.com/articles/home-depot-ceo-probe-continues-into-possible-data-breach-1409844745
[32] Ponemon Institute, *2014 Cost of Data Breach Study: United States* 1-2 (May 2014).

identifiable health information." The Gramm-Leach Bliley Act (GLBA) concerns "personally identifiable financial information." The Privacy Act of 1974 protects an "identifying particular assigned to an individual." The Freedom of Information Act (FOIA) protects "personal identifying information," and the Family Educational Rights and Privacy Act (FERPA) protects "personally identifiable information."

Individual states have different definitions of "personal information." For example, Minnesota's notification statute, Minn. Stat. § 325E.61, defines "personal information" as a person's name in combination with a person's Social Security number, driver's license or identification card number, account number or credit or debit card number in combination with any required security code, access code, or password permitting access to an individual's financial account. Effective January 1, 2014, California became the first state to expand the definition of "personal information" to include online account log-in or access data, such as a "user name or email address, in combination with any required security question and answer that would permit access to an online account."[33] It is likely that other states will similarly expand the definition of "personal information."[34]

B. Regulated entities

The various federal and state laws delineate those who must comply with them. HIPAA, by way of its Security Rule, requires health care "covered entities" to maintain safeguards that protect electronic "protected health information," including standards for passwords, firewalls, backups, and transmission security.[35] Entities must have agreements with "business associates" regarding the handling of electronic protected health information. A "business associate" is a person, other than an employee, who assists a covered entity with claims processing, billing, or handling, or provides the entity legal, actuarial, accounting, or certain other services that involve disclosure of individually identifiable health information.[36] HIPAA's Privacy Rule protects against unauthorized uses and disclosure of protected health information.[37] Failure to comply with HIPAA's provisions may result in a civil fine based on a tiered system, up to $50,000/violation and up to $1.5 million for violations of an identical requirement during a calendar year. There are criminal penalties if the offense is made under false pretenses or there is intent to sell or obtain other gain, fines up to $250,000 and/or imprisonment up to 10 years.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) extends HIPAA to the "business associates" of HIPAA "covered entities," subjecting them

[33] Cal. Civ. Code § 1798.29(g)(2), -.82(h)(2).
[34] *See* Fla. S.B. 1524, effective July 1, 2014, creating Fla. Stat. Ann. § 501.171, including the same expansive definition of "personal information" as California.
[35] 45 C.F.R. § 164.300, *et seq.*
[36] 45 C.F.R. § 160.103.
[37] 45 C.F.R. § 164.500, *et seq.*

to civil and criminal liability.[38] The Act has notification requirements for breaches of "unsecured protected health information," and specifies ways to render protected information "secured."

The GLBA requires financial institutions to protect customer information. GLBA's Safeguards Rule requires financial institutions to have a written information security plan.[39] Penalties under the GLBA include a fine up to a $100,000 per violation, up to a $10,000 fine for an entity's officers and directors for each violation, and imprisonment up to 5 years and/or a fine.

The Fair and Accurate Credit Transactions Act (FACTA) prohibits both the printing of more than the last 5 digits of a credit or debit card number and the printing of the card's expiration date on credit and debit card receipts.[40] The Act's Disposal Rule requires that anyone collecting or possessing consumer information for business purposes must properly dispose of it by using "reasonable measures" to protect against unauthorized access or use of the information in connection with the disposal.[41] Consumers may recover actual and statutory damages sustained as a result of a violation.

The Federal Trade Commission's Health Breach Notification Rule requires certain entities not covered by HIPAA to notify customers if there is a breach of unsecured individually identifiable electronic health information.[42] Notice must be given to affected people within 60 days of discovery, and to the FTC (within 10 days if the breach involves 500 people or more). The FTC's Red Flags Rule requires "financial institutions" and "creditors" to maintain an identity theft prevention program.[43]

The Electronic Communications Privacy Act (ECPA), Wiretap Act, and Stored Communications Act make it illegal to intercept stored or transmitted electronic communications, or intentionally use or disclose such communications without authorization.[44] Violations might result in imprisonment up to 5 years and fines up to $250,000.

State statutes and rules also apply to defined entities and protected information. For instance, Minnesota's Data Retention Act does not permit merchants to retain credit card security codes, PIN numbers, or the full contents of magnetic strips after a transaction has been authorized; for debit transactions requiring a PIN number, merchants may retain the information for 48 hours after authorization.[45] Merchants are liable for violations caused by their third-party service providers.

[38] 42 U.S.C. § 300jj, *et seq.*; § 17901, *et seq.*
[39] 15 U.S.C. §§ 6801-6809, 6821-6827.
[40] 15 U.S.C. § 1681.
[41] 16 C.F.R. § 682.
[42] 16 C.F.R. § 318.
[43] 16 C.F.R. § 681.
[44] 18 U.S.C. §§ 2510-2521, 2701-2710.
[45] Minn. Stat. § 325E.64.

C. Notification

1. Federal requirements

There is no comprehensive federal law on data-breach notification. The HITECH Act requires notice to individuals when it is reasonably believed that a breach of unsecured personal health information has occurred. Notice must be given without unreasonable delay, but no later than 60 days after discovery of the breach. If a breach affects more than 500 residents of a state, notice must also be given to prominent media outlets in the state. Notice must also be given to the Secretary of the U.S. Department of Health and Human Services.

The Federal Trade Commission's Health Breach Notification Rule (16 C.F.R. § 318) requires certain entities not covered by HIPAA to notify customers if there is a breach of unsecured individually identifiable electronic health information. Notice must be given to affected people within 60 days of discovery, and to the FTC (within 10 days if the breach involves 500 people or more).

In contrast, the GLBA does not have express notification provisions, but its security guidelines recommend implementing a risk-based response program, which have been interpreted as including customer notification where misuse of information has occurred or is reasonably possible.

2. State requirements

Forty-seven states and the District of Columbia have legislation requiring notification of security breaches involving personal information.[46] Only Alabama, New Mexico, and South Dakota lack such legislation. Obligations vary from state to state. State data-breach laws specify what constitutes a breach, and the timing, manner, and content of a notice of a breach.[47] For instance, Minnesota requires that any person or entity doing business or that owns or licenses data including "personal information" must disclose any discovery of a breach of the security system by notifying Minnesota residents "in the most expedient time possible" that unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.[48] And notification must be made to the owner or licensee of the information.[49] If notification of more than 500 persons is required, notice must be given within 48 hours to all

[46] *See* National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (also attached as Appendix, *infra*).
[47] *E.g.*, Ariz. Rev. Stat. Ann. § 44-7501.L (defining "breach" as "an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual").
[48] Minn. Stat. § 325E.61, subd. 1(a).
[49] *Id.*, subd. 1(b).

consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.[50]

States may permit a business to notify affected individuals of a breach by written notice, electronic notice, telephonic notice, or substitute notice if the cost exceeds a statutory amount.[51] And some states require that covered entities notify not only affected individuals of a breach, but also the state attorney general or a state agency in the event of a data breach.[52] A handful of states permit a private right of action for failure to comply with breach notification requirements.

The takeaway is that in the event of a breach, entities must diligently inquire into their obligations to notify necessary individuals and other entities under both state and federal law, and meet the who, what, when, where, and why requirements. Claim handlers involved with data-breach situations should be aware of the various sources of potential liability for insureds under federal and state statutes and rules.

III. LITIGATION

A. Litigants

The most common form of litigation arising out of data breaches is, unsurprisingly, based on claims from affected individuals, whose information was stolen or put at risk.[53] Nevertheless, litigation brought by government entities has become more frequent with the number and scope of data breaches. For instance, the FTC has been very active in bringing enforcement actions based on alleged violations of Section 5 of the FTC Act, which prohibits "acts or practices in or affecting commerce that are 'unfair' or 'deceptive.'"[54] The FTC's actions have generally resulted in settlements.[55] Recently, however, in *Federal Trade Commission v. Wyndham Worldwide Corp.*, the FTC brought an action under Section 5(a) of the FTC Act against Wyndham entities, asserting that they had failed "to maintain reasonable and appropriate data security for consumers' sensitive personal information," amounting to an unfair and deceptive practice.[56] For the first time, the defendant in a suit brought by the FTC challenged the FTC's authority to assert an unfairness claim in the data-security context.[57] The court confirmed, on a motion to dismiss, that the FTC did have such authority under the FTC Act to enforce it with respect to an entity's

[50] *Id.*, subd. 2.
[51] *E.g.*, Ariz. Rev. Stat. § 44-7501.A-D.
[52] *E.g.*, Cal. Civ. Code § 1798.29(e) (requiring notice to state attorney general where notification is required in the event of a security breach involving more than 500 California residents) & -.82(f) (same); N.Y. Gen. Bus. § 899-aa.8 & N.Y. Tech. Law § 208.7.
[53] *E.g.*, *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014).
[54] 15 U.S.C. § 45(a).
[55] *E.g.*, *In re Myspace LLC*, No. C-4369 (F.T.C. Aug. 13, 2012) (Myspace settled with the FTC in September 2012, requiring Myspace to implement a comprehensive privacy program with assessments for the next 20 years, and barring it from future misrepresentations about privacy practices; the FTC charged Myspace with violating its privacy policy by providing advertisers with a unique identifier for users that viewed certain Myspace pages); *United States v. RockYou*, No. 12-CV-1487 (N.D. Cal. Mar. 26, 2012) (gaming company RockYou settled with the FTC in March 2012, agreeing to pay a $250,000 penalty and implement a data security program after hackers accessed data from RockYou's 32 million users in 2009; RockYou violated the Children's Online Privacy Protection Act Rule by collecting personal information of children, and violating the FTC Act by indicating it did not collect such information when it did).
[56] 2014 WL 1349019, at *1 (D.N.J. Apr. 7, 2014).
[57] *Id.*

data-security measures because failure to protect against repeated cyber attacks can constitute an unfair and deceptive practice.[58] This court approval will likely lead to even more FTC enforcement actions.

In addition to claims from affected individuals or government entities, in situations involving credit cards, a retailer might also face suits from banks issuing the credit cards in order to recover costs involved with cancelling and reissuing cards.[59] Shareholders also have now started asserting derivative actions against companies' directors and officers based on breach of fiduciary duty, waste of corporate assets, abuse of control, gross mismanagement, and other claims in efforts to hold a company's officials liable for damages resulting from a data breach.[60] Shareholder derivative actions are a recent trend that will likely continue. They allow plaintiffs to avoid one of the primary problems in data-breach class actions—having to prove that class members suffered common damages as a result of a data breach of theft of personal information.[61]

B. Injury and Standing

Although litigants and data breaches abound, litigants face significant hurdles in prevailing on their claims. A key consideration in any data-breach litigation is whether the claimant has standing. Standing concerns whether a party has a "right to make a legal claim or seek judicial enforcement of a duty or right."[62] In U.S. federal court, where a large number of data-breach lawsuits are venued, plaintiffs must establish Article III standing under the U.S. Constitution. In order to establish Article III standing, a plaintiff must show three things: "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[63]

1. Injury in fact.

Data-breach plaintiffs have asserted various ways in which they have been injured by a data breach in efforts to prove standing, including:

1. Actual identity theft with misuse of personal information,[64]
2. Increase risk of harm,[65]

[58] *Id.* at *8-9.
[59] *E.g.*, *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 918 N.E.2d 36, 39 (Mass. 2009).
[60] *E.g.*, *Palkon v. Holmes*, No. 2:14-cv-01234 (D.N.J. May 2, 2014) (concerning Wyndham Hotels' three data breaches that resulted in the theft of 619,000 payment card account numbers); *Kulla v. Target Corp.*, No. 14-cv-203 (D. Minn., filed Jan. 21, 2014) (concerning Target's 2013 Black Thursday breach involving 40 million credit and debit cards); *Collier v. Target Corp.*, No. 14-cv-266 (D. Minn., filed Jan. 29, 2014) (same). A shareholder derivative action was also brought in *Louisiana Municipal Police Employees Retirement Fund v. Alvarez*, No. 5620-VCN (Del. Ch. July 2, 2010), but the case settled early in litigation.
[61] *See* Fed. R. Civ. P. 23(a).
[62] *Black's Law Dictionary* 1442 (8th ed. 2004).
[63] *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000).
[64] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012).

3. Cost to mitigate increased risk,[66]
4. Loss of privacy,[67]
5. Deprivation of value of personal information,[68]
6. Diminished value of products and services.[69]

a. Actual identity theft with misuse of personal information

On one end of the standing spectrum are instances where a data-breach plaintiff alleges actual identity theft with misuse of personal information. Such instances sufficiently establish standing.[70]

b. Increase risk of harm

It is far more common, however, that plaintiffs allege only an increase of risk of harm of identity theft or fraud, not actual identity theft. Courts have split on the issue of whether increased risk of harm establishes standing.[71]

In 2013, the U.S. Supreme Court in *Clapper v. Amnesty International USA* analyzed the contours of standing in the context of threatened injury, though not in the data-breach context.[72] In *Clapper*, the plaintiffs challenged the Foreign Intelligence Surveillance Act of 1978, which allowed surveillance of people who were not "United States persons" and who were believed to be located outside the U.S.[73] The plaintiffs were various individuals who argued they would likely be monitored under the Act because they worked with foreign individuals who would be targets of surveillance under the Act.[74] When their standing was challenged, plaintiffs argued that they had sufficiently alleged an "injury-in-fact" based on: (1) the "objectively reasonable likelihood" that their communications would at some point be targeted under the Act; and (2) the fact that they had taken personal costly measures to protect the confidentiality of the conversations with clients.[75]

The Supreme Court rejected plaintiffs' arguments, stating that although it may be "objectively reasonable" that their communications might at some point be intercepted under the

---

[65] *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-CV-118, 2014 WL 689703, at *5 (S.D. Ohio Feb. 10, 2014).
[66] *Id.*
[67] *Id.* at *9.
[68] *Id.* at *10.
[69] *Katz v. Pershing, LLC*, 672 F.3d 64, 76 (1st Cir. 2012); *McLoughlin v. People's United Bank, Inc.*, CIVA 308CV-00944 VLB, 2009 WL 2843269, at*3 (D. Conn. Aug. 31, 2009).
[70] *E.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012).
[71] *Compare Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (mere increased risk of identity theft insufficient to establish standing), and *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (allegations only of an increased risk that someone might access personal information was insufficient for standing), *with Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (finding injury in fact where unauthorized person accessed but had not yet misused plaintiffs' personal information), and *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007) (finding injury in fact where plaintiffs alleged increased risk of data theft after personal information had been accessed by a sophisticated hacker), and *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 958 (S.D. Cal. 2012) (finding standing based on increased risk of future harm).
[72] 133 S. Ct. 1138 (2013).
[73] *Id.* at 1142.
[74] *Id.*
[75] *Id.* at 1143, 1145-46.

Act, they had failed to show that the "threatened injury" was "*certainly impending*."[76] The Court noted that a "speculative chain of possibilities ... based on potential future surveillance" was not enough, and declined to "abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors."[77] The standard set forth in *Clapper* that an injury must be "certainly impending" led to several courts applying a "certainly impending" standard in the context of increased risk of identity theft because of a data breach.[78]

The Supreme Court, however, recently came out with a unanimous opinion in *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334 (June 16, 2014), which clarified that *Clapper*'s "certainly impending" standard had not overruled prior Supreme Court cases requiring only that there be a "substantial risk" that the harm will occur: "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony*'s clarification of *Clapper* has resulted in one court concluding that the two Supreme Court cases ultimately do not affect whatever the particular Circuit's law on standing in the data-breach context had been before *Susan B. Anthony* and *Clapper* were decided.[79] Therefore, when analyzing standing in an increased risk-of-harm situation, it is best to consider any prior decisions from the relevant Circuit Court of Appeals.[80]

c. Cost to mitigate increased risk

Similarly, some courts have held that credit monitoring or costs associated with mitigating or preventing future harm do not confer standing.[81] The Supreme Court in *Clapper* ruled out such argument when it stated that proactive measures based on "fears of … future harm that is not certainly impending" do not create an injury in fact, even where such fears are not unfounded.[82] Stated differently, the Court held that plaintiffs cannot create standing by "inflicting harm on themselves" to prevent speculative injury.[83] Although the "certainly impending" standard from *Clapper* is not necessarily the applicable standard in light of *Susan B. Anthony*, the rule to be gleaned from *Clapper* is that if there is no injury in fact sufficient to establish standing based on an increased risk of harm, then preventive costs do not constitute an

[76] *Id.* at 1147 (emphasis added).
[77] *Id.* at 1150.
[78] *E.g.*, *Strautins v. Trustwave Holdings, Inc.*No. 12-9115, 2014 WL 960816, at *4 (N.D. Ill. Mar. 12, 2014) (concluding that after *Clapper*, "the mere fact that the risk has been increased does not suffice to establish standing" because the potential injury was based on too many variables); *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-CV-118, 2014 WL 689703, at *5 (S.D. Ohio Feb. 10, 2014); *Polanco v. Omnicell, Inc.*, No. 13-1417, 2013 WL 6823265, at *14 (D.N.J. Dec. 26, 2013); *In re Barnes & Noble Pin Pad Litg.*, No. 12-cv-8617, 2013 4759588, at *3 (N.D. Ill. Sept. 3, 2013). *But see In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, MDL 11MD2258 AJB MDD, 2014 WL 223677, at *8-9 (S.D. Cal. Jan. 21, 2014) (concluding that *Clapper* was consistent with prior Ninth Circuit case law concluding that plaintiffs had alleged standing sufficient to withstand motion to dismiss based on plausible allegations of a "credible threat" of impending harm based on disclosure of personal information following an intrusion).
[79] *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500, at *5-6 (N.D. Ill. July 14, 2014).
[80] *E.g.*, Third Circuit: *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (increased risk of harm was too speculative to confer standing where it was "not known whether the hacker read, copied, or understood the data"); Seventh Circuit: *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632 (7th Cir. 2007) (finding standing because "the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious"); Ninth Circuit: *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010) (stating that the "possibility of future injury may be sufficient to confer standing on plaintiffs; threatened injury constitutes 'injury in fact'").
[81] *Reilly*, 664 F.3d at 46.
[82] *Clapper*, 133 S. Ct. at 1151.
[83] *Id.*

injury sufficient for standing either.[84] Therefore, "the cost of precautionary measures … provides standing only if the underlying risk of identity theft is sufficiently imminent to constitute an injury-in-fact."[85]

d. Loss of privacy

Courts have also disagreed on whether plaintiffs have standing based on allegations that their privacy has been invaded by a data breach. The deciding factor for the courts has been whether there are allegations that the plaintiffs' information had been *accessed* or *used*.[86] Even if a court finds standing because of alleged injury based on loss of privacy, it might conclude that plaintiffs have standing for invasion of privacy claims, but not negligence or other claims.[87]

e. Deprivation of value of personal information

Plaintiffs have been creative and also asserted that they have standing because they were injured by a loss of value of personal information.[88] Courts, however, have not been receptive to such arguments. Some courts have concluded that personal information has no inherent monetary value.[89] Other courts have concluded that it is unclear how personal information had been devalued by a breach or a plaintiff deprived of the economic value of such information, and rejected arguments for standing based on deprivation or devaluation of personal information.[90]

f. Diminished value of products and services

In addition, plaintiffs have argued that part of payments made to defendants went to security measures to protect personal information, but defendants' failure to employ adequate security measures resulted in overpayment or diminished value of purchased products and services.[91] But this argument has been rejected on the basis that there were no allegations that a specific amount was allocated for specific security measures.[92]

---

[84] *See, e.g.*, *Reilly*, 664 F.3d at 46 ("Appellants' alleged time and money expenditures to monitor their financial information do not establish 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'").
[85] *Moyer*, 2014 WL 3511500, at *7 n.1 (citing *Clapper*).
[86] *E.g.*, *Katz v. Pershing, LLC*, 672 F.3d 64 (dismissing privacy claim for lack of standing where information had not been viewed by a third party); *Strautins*, 2014 WL 960816, at *7; *In re: Sci. Applications Int'l Corp (SAIC) Backup Tape Data Theft Litig.*, MDL No. 2360, 2014 WL 1858458, at *9-10 (D.D.C. May 9, 2014) (plaintiffs that alleged that their data had been accessed and used had standing, but no standing for plaintiffs who contended neither that their information had been viewed "nor that their information has been exposed in a way that would facilitate easy, imminent access").
[87] *Galaria*, 2014 WL 689703, at *10 (concluding that allegations of personal information being stolen and disseminated to criminals conferred standing for state law invasion of privacy claims, but not for negligence and bailment claims).
[88] *SAIC Backup Tape Litig.*, 2014 WL 1858458, at *10.
[89] *E.g.*, *Willingham v. Global Payments, Inc.*, No. 1:12–CV–1157–RWS, 2013 WL 440702, at *6 (N.D. Ga. Feb. 5, 2013).
[90] *E.g.*, *SAIC Backup Tape Litig.*, 2014 WL 1858458, at *10; *In re Barnes & Noble Pin Pad Litig.*, No. 12–cv–8617, 2013 WL 4759588, at *5 (N.D. III. Sept. 3, 2013) (concluding that "Plaintiffs' claim of injury in the form of deprivation of the value of their [personal information] is insufficient to establish standing. Actual injury of this sort is not established unless a plaintiff has the ability to sell his own information and a defendant sold the information." (internal citations omitted)).
[91] *E.g.*, *In re Barnes & Noble*, 2013 WL 4759588, at *5.
[92] *E.g.*, *Katz v. Pershing, LLC*, 672 F.3d 64, 72 (1st Cir. 2012).

In sum, data-breach plaintiffs have obstacles in showing an injury in fact sufficient for standing to assert their claims in litigation. Actual identity theft and fraudulent use of personal information suffices for standing. And depending on the jurisdiction, increased risk of future harm might also suffice. Other arguments have not been successful where the jurisdiction does not recognize increase of risk of harm as establishing standing.

2. Causation

Besides showing an injury in fact, plaintiffs must also show that an injury is fairly traceable to the challenged action of the defendant.[93] In other words, for standing, data-breach plaintiffs must show that the breach caused the injury, though an injury that is indirectly caused by a defendant's actions satisfies the fairly traceable requirement.[94] Courts have concluded that data-breach plaintiffs have not shown their injury is traceable to the breach where they are unable to show that the identity theft was based on information obtained in the breach.[95] For instance, there is an insufficient causal connection where the information obtained from a data breach is not necessarily the information used to perpetrate identity theft.[96] In contrast, there is likely a sufficient causal connection where identity theft was based on information specifically contained in the data breach.[97]

C. Causes of Action

Even if data-breach plaintiffs establish standing, that does not mean they will succeed on their claims. There is a distinction between whether an injury results in standing for a litigant and whether the injury is grounds for a legal claim upon which relief may be granted. For standing under Article III, the injury must be an interest "that the law protects when it is *wrongfully* invaded."[98] This is "different from requiring [plaintiffs] to establish a *meritorious* legal claim" as a precondition for standing.[99] In other words, even if a party has standing because it has shown an "injury in fact," it still might not have stated a claim recognizable by law.

1. Tort

Data-breach plaintiffs often assert tort claims in data-breach litigation, and primarily, negligence claims. For negligence claims, plaintiffs must show that (1) defendants owed plaintiffs a duty, (2) a breach of that duty by conduct falling below the applicable standard of care, (3) compensable injury, (4) proximately caused by the breach of duty.[100]

---

[93] *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000).
[94] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012).
[95] *E.g.*, *SAIC Backup Tape Litig.*, 2014 WL 1858458, at *11-12.
[96] *E.g.*, *id.*
[97] *E.g.*, *Resnick*, 693 F.3d at 1324; *Lambert v. Hartman*, 517 F.3d 433, 437-38 (6th Cir. 2008).
[98] *Aurora Loan Servs., Inc. v. Craddieth*, 442 F.3d 1018, 1024 (7th Cir. 2006).
[99] *Id.*
[100] *E.g.*, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 635 (7th Cir. 2007).

Negligence claims have generally been unsuccessful because of lack of compensable injury. The cases that have found a cognizable injury for standing purposes have generally concluded that the claimed damages for mere identity theft exposure and credit monitoring are not compensable under applicable state law.[101] One Circuit Court of Appeals, however, has concluded that credit monitoring and identity theft insurance were compensable damages where there had been a large-scale criminal operation with a deliberate taking of credit card information and over 1800 unauthorized charges.[102]

In addition, courts have generally held that the economic loss doctrine bars recovery under data-breach plaintiffs' negligence claims.[103] Under the economic loss doctrine, plaintiffs are barred from recovery unless they can establish that their injuries due to defendants' negligence involved physical harm or property damage, and are not purely economic loss.[104] The purpose is to limit a plaintiff to seeking recovery of purely economic losses to contractual remedies.[105] Thus, some courts have held that the doctrine barred data-breach plaintiffs' claims because there was no physical injury or property damage. The precise application of the economic loss doctrine, however, varies from state to state. Recently, the Fifth Circuit Court of Appeals concluded that, under New Jersey law, the economic loss doctrine did not bar negligence claims by plaintiff credit-card-issuing banks that incurred losses associated with replacing credit cards, provided consumers with monitoring services, and suffered losses from fraudulent use of the stolen data, because the plaintiffs were a limited, identifiable collection of claimants the defendant knew or had reason to know would likely suffer damages from a breach.[106] Thus, like standing, the applicability of the economic loss doctrine depends on the jurisdiction and the particular facts of a case.

Data-breach plaintiffs must also show that defendants owed them a duty. Courts have concluded that no such duty exists where there was no direct relationship between defendants and plaintiffs.[107]

In addition to general negligence claims, plaintiffs have asserted a variety of tort claims based on data breaches, including:

- Negligence per se (based on violations of various statutes)
- Negligent misrepresentation
- Invasion of privacy
- Conversion
- Tortious interference

[101] *Id.* at 639; *Krottner v. Starbucks Corp.*, 406 Fed App'x 129, 131 (9th Cir. 2010).
[102] *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 165 (1st Cir. 2011).
[103] *E.g.*, *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498-99 (1st Cir. 2009) (credit-card issuing bank's negligence claim against retailer whose system was breached was barred by the economic loss doctrine because there was no physical destruction of property); *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 918 N.E.2d 36, 46-47 (Mass. 2009).
[104] *Id.*
[105] *Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 423 (5th Cir. 2013).
[106] *Id.* at 426.
[107] *E.g.*, *Willingham v. Global Payments, Inc.*, 1:12-CV-01157, 2013 WL 440702, at *18 (N.D. Ga. Feb. 5, 2013).

2. Contract

In addition to tort claims, data-breach plaintiffs often bring contractual claims. For a breach of contract claim, plaintiffs must show (1) the existence of a contract between the plaintiff and defendant, (2) the rights of the plaintiff and obligations of the defendant under the contract, (3) a defendant's breach of the contract, and (4) a plaintiff's damages.[108] Such claims rest on the premise that a defendant contractually promised to protect personal information, but breached such promise. Courts have held that a company's statements about its data security do not amount to an enforceable contract.[109]

Because there are often no grounds for breach of an express contract, data-breach plaintiffs often assert claims for breach of an implied contract, such that a company experiencing a data breach impliedly contracted to safeguard data. Such arguments have had mixed results. Courts have split on whether a plaintiffs' purchase of goods from a merchant constituted an implied contract to take reasonable measures to protect personal information and not permit unauthorized access to the data.[110] But where plaintiffs do not give their personal information directly to defendants, a court will likely find no implied contract to safeguard personal information.[111]

In order to overcome the obstacle of the lack of direct relationship with a defendant, data-breach plaintiffs might assert that they should be considered "third-party beneficiaries" of the defendant's contracts with others whereby the defendant agrees to safeguard personal information. Such claims have generally been dismissed.[112]

Plaintiffs have also asserted claims for unjust enrichment, which requires them to show that they conferred a benefit on a defendant, the defendant had knowledge of the benefit, accepted the benefit, and circumstances are such that it would be inequitable to retain the benefit without paying fair value.[113] This has generally been asserted where plaintiffs contend that they paid money to defendants for services or a product, and part of such payment was for

[108] *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009).
[109] *In re Zappos.com, Inc.*, MDL No. 2357, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013).
[110] *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 158-59 (1st Cir. 2011) (denying motion to dismiss implied contract claim of grocery store customers whose financial data was allegedly stolen by third parties, resulting in widespread fraudulent charges, because "a jury could reasonably conclude [ ] that an implicit agreement [by a store] to safeguard [customers'] data is necessary to effectuate the contract" existing between them); *In re Zappos*, 2013 WL 4830497, at *3 (dismissing claim for an implied contract between customer and merchant where customer simply agreed to pay money for goods);
[111] *See, e.g.*, *Willingham*, 2013 WL 440702, at *21.
[112] *See, e.g.*, *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498-99 (1st Cir. 2009) (credit-card issuing bank's contract claim failed because the bank was not a third-party beneficiary of the contracts between the retailer and credit-card organizations); *Willingham*, 2013 WL 440702, at *19-20 (customer plaintiffs were not intended third-party beneficiaries of the agreement between merchant and payment processor); *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 918 N.E.2d 36, 43-44 (Mass. 2009) (credit unions that issued credit cards were not third-party beneficiaries of the acquiring bank's contracts with Visa and MasterCard).
[113] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012).

administrative costs of data management and security.[114] Some states, however, do not recognize unjust enrichment as a separate cause of action.[115]

Plaintiffs have also tried to assert a cause of action of bailment.[116] But such arguments have been rejected because defendants generally are not involved with the data breach, and did not convert or unlawfully retain and possess plaintiffs' personal information.[117]

3. Statutory law

In addition to common law causes of action, plaintiffs have and will assert statutory claims. For example, in the liability litigation involving Sony's 2011 PlayStation breach of millions of customers, plaintiffs alleged violations of California's (1) Unfair Competition Law, (2) False Advertising Law, and (3) Consumers Legal Remedies Act.[118] In Barnes & Noble's 2012 data breach affecting sixty-three stores in nine states, plaintiffs brought a class action alleging violations of (1) the Illinois Consumer Fraud and Deceptive Business Practices Act, (2) the California Security Breach of Notification Act, and (3) California's Unfair Competition Act. And in the consolidated class actions involving Schnuck Market's 2013 data breaches, plaintiffs' brought consolidated class actions asserting a variety of claims, including violations of: (1) the Illinois Personal Information Protection Act, (2) the Illinois Consumer Fraud and Deceptive Business Practices Act, (3) the Illinois Consumer Fraud Act, (4) the Stored Communications Act, and (5) the Missouri Merchandising Practices Act.[119] Thus, defendants and insurers must be cognizant of the wide variety of state and federal statutory claims plaintiffs might assert.

D. Applicable Law

The foregoing discussion of standing and causes of actions illustrates that jurisdictions differ in deciding issues arising in data-breach litigation. One jurisdiction might permit claims that another would dismiss. This heightens the importance of defendants attempting to identify law that could be applied that is most favorable to them. Simply because a suit is brought in a particular court does not mean that the court will apply that jurisdiction's law. For example, in *Lone Star National Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 423 (5th Cir. 2013), a case originally filed in the Federal District Court for the Southern District of Texas, the parties disagreed about whether Texas law or New Jersey law should be controlling. The economic doctrine as applied in Texas would have precluded plaintiffs' negligence claims, whereas New Jersey law did not. The plaintiffs convinced the court that it should apply New Jersey law for purposes of the motion to dismiss, and such law did not bar their negligence

[114] *Id.* (denying motion to dismiss unjust enrichment claim).
[115] *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012) (dismissing unjust enrichment claim because California does not recognize it as a separate cause of action).
[116] *See, e.g.*, *id.*
[117] *See id.*
[118] *Id.* at 964.
[119] *In re: Schnuck Markets, Inc., Customer Data Sec. Breach Litig.*, 978 F. Supp. 2d 1379 (M.D.L. 2013).

claims.[120] Therefore, a key component to any litigation is determining what law might apply and what law is most favorable to the party's arguments.

IV. Conclusion

Data-breach plaintiffs have been largely unsuccessful in overcoming motions to dismiss for lack of standing or failure to state a claim under applicable law. But given the number and ever-increasing size of the breaches, plaintiff lawyers will continue to look for ways to strike a large victory. Data-breach litigation will continue to evolve with plaintiffs trying new theories of liability. Carriers and defense counsel must pay close attention to developments in the law and the particular facts of a data-breach claim.

[120] *Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 426-27 (5th Cir. 2013).

APPENDIX

Table of State Security Breach Notification Laws

National Conference of State Legislatures, *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 44–7501
Arkansas	Ark. Code Ann. § 4-110-101 et seq.
California	Cal. Civ. Code §§ 1798.29, 1798.80 et seq.
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen. Stat. § 36a-701b
Delaware	Del. Code Ann. tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. § 817.5681
Georgia	Ga. Code Ann. § 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. §§ 487N-1 et seq.
Idaho	Idaho Code Ann. § 28-51-104 to -107
Illinois	815 Ill. Comp. Stat. 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 et seq.; 24-4.9 et seq.
Iowa	Iowa Code §§ 715C.1, 715 C.2
Kansas	Kan. Stat. Ann. §§ 50-7a01 et seq.
Kentucky	2014 H.B. 54, H.B. 232
Louisiana	La. Rev. Stat. Ann. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10, § 1347 et seq.
Maryland	Md. Code Ann., Com. Law § 14-3501 et seq.301 to -1308
Massachusetts	Mass. Gen. Laws ch. 93H-1 et seq.
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code Ann. § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code Ann. §§ 2-6-504; 30-14-1701 et seq.
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21
New Jersey	N.J. Stat. Ann. § 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa; N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat § 75-61, 75-65
North Dakota	N.D. Cent. Code § 51-30-01 et seq.
Ohio	Ohio Rev. Code Ann. §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. tit. 74, § 3113.1 and tit. 24, §§ 161–166
Oregon	Or. Rev. Stat. § 646A.600 et seq.
Pennsylvania	73 Pa. Stat. Ann. § 2301 et seq.
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.
South Carolina	S.C. Code Ann. § 39-1-90
Tennessee	Tenn. Code Ann. § 47-18-2107
Texas	Tex. Bus. & Com. Code Ann. § 521.001, 521.053 § 37.007(b)(5)
Utah	Utah Code Ann. §§ 13-44-101 et seq.
Vermont	Vt. Stat. Ann. tit. 9, § 2430, 2435
Virginia	Va. Code Ann. §§ 18.2-186.6, 32.1-127.1:05

Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia	W. Va. Code § 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98 et seq.
Wyoming	Wyo. Stat. Ann. §§ 40-12-501 et seq.
District of Columbia	D.C. Code § 28- 3851 et seq.

9866642