INSIDE THE MINDS

Privacy and Surveillance Legal Issues

Leading Lawyers on Navigating Changes in Security Program Requirements and Helping Clients Prevent Breaches

ASPATORE

Private Data Security Breach Litigation in the United States

Douglas H. Meal
Partner
with
David T. Cohen
Associate

Ropes & Gray LLP

ASPATORE

Introduction

As then-Federal Bureau of Investigation (FBI) Director Robert Mueller recently put it, "[T]here are only two types of companies: those that have been hacked and those that will be."[1] In recent years, more and more corporations have disclosed that they have been a victim of a data security breach, often as the result of sophisticated hackers (frequently in foreign countries) penetrating their computer systems and potentially stealing information about individuals such as the company's customers or employees.

Although data security breaches are now commonplace, those breaches where personal information is stolen or put at risk of being stolen often trigger legal claims by private plaintiffs seeking to characterize the breach as the result of unreasonable, lax measures by the breached company in protecting the personal information in question. In defending many data security breach victims against such claims, we have seen the range of contentions these plaintiffs make, and how courts have addressed them. As we explain below, such plaintiffs frequently struggle to plead and prove that the data security breach resulted from the victim's breach of its legal obligations, as opposed to an unfortunate perpetration of computer crime by third parties, and/or that any breach of legal obligations caused any recoverable injury.[2] As plaintiffs' lawyers continue to look for ways to overcome these difficulties, all data security practitioners should pay close attention to further developments in the case law and their implications for companies that collect or use information about individuals.

Potential Litigants against Companies that Have Suffered Data Security Breaches

Companies that suffer data security breaches can face claims by a wide variety of private litigants. The most common private litigant against a corporate victim of a data security breach is the individual or individuals, such as a

[1] *See* Prepared Remarks of Robert S. Mueller, Director, FBI, RSA Cyber Security Conference (Mar. 1, 2012), http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[2] We address here only claims by private parties. Victims of data security breaches can also face investigations or lawsuits by government agencies seeking to enforce consumer protection laws. We also focus here on data security breaches exposing information about individuals, as opposed to theft of trade secrets or other types of information exposure.

consumer or employee, whose data was allegedly stolen or may have been placed at risk of being stolen from the company during the breach.[3]

If payment card data was potentially stolen, the company may face claims not only by the cardholders whose card information was involved,[4] but also by the banks and credit unions that issued the cards, which seek compensation for the cost of reimbursing their customers for fraudulent charges, re-issuing cards, and monitoring compromised accounts.[5] Insurers who have reimbursed financial institutions for such losses may likewise seek to recover them from the breached company.[6] In addition, card brands such as Visa and MasterCard may impose fines for violating their rules governing data security practices and/or assessments to pay the financial institutions that issued the compromised cards for losses they claim to have incurred.[7]

A breached company may also face claims by other plaintiffs, including by shareholders under federal securities laws for allegedly inadequate disclosures of data security risks.[8]

Threshold Issues Relating to Injury and Damages

Private civil actions against companies that have suffered data security breaches raise a panoply of issues, but none more prevalent or decisive than those relating to injury and damages. This is because most plaintiffs in data

---

[3] *Bell v. Blizzard Entm't, Inc.*, No. 12-cv-09475, at *3 (C.D. Cal. July 11, 2013) (suit by consumers); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d Cir. 2011) (suit by employees).
[4] *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164 (1st Cir. 2011).
[5] *Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421 (5th Cir. 2013); *In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 491-2 (1st Cir. 2009).
[6] *See Cumis Ins. Soc., Inc. v. Merrick Bank Corp.*, CIV07-374-TUC-CKJ, 2008 WL 4277877, at *1 (D. Ariz. Sept. 18, 2008).
[7] *See Genesco, Inc. v. Visa U.S.A. Inc.*, 3:13CV202, 2013 WL 3790647, at *1 (M.D. Tenn. July 18, 2013). In many instances, such as where the victim of the breach is a merchant, card brands such as Visa and MasterCard do not share a direct contractual relationship with the breached company. Instead, "acquiring banks" contract with Visa and MasterCard to become members of the payment card systems, and then these banks contract with merchants to sponsor their participation and enable them to accept card payments. Thus, when a merchant suffers a breach, the card brands generally impose fines and assessments directly on the acquiring banks, who then assert claims against their merchant customers for reimbursement. *Id.*
[8] *See, e.g., In re Heartland Payment Sys., Inc. Sec. Litig.*, CIV. 09–1043, 2009 WL 4798148, at *1-2 (D.N.J. Dec. 7, 2009).

security actions have not experienced any actual misuse or fraud resulting from the breach, but instead premise their claims on alternative theories of injury, such as the risk of harm. Judicial decisions addressing data security claims have placed clear limitations on the types of injuries the law will remedy. Further, even where there is injury sufficient to state a claim, a plaintiff also must show causation, including that the harm was the result of the particular breach at issue. With the widespread use of online storefronts, social media, and the countless other interactions in which consumers today share their information in the digital realm, and with the very frequency of breaches themselves, connecting any one incident of misuse to the specific breach at issue can prove challenging. Finally, otherwise recoverable damages may be foreclosed under principles specific to particular causes of action, such as the economic loss doctrine.

Added together, injury and damages issues account for a significant portion of the litigation that takes place in the data security space, and present plaintiffs with complex challenges that can prove difficult to overcome.

Cognizable Injury

Common to almost every cause of action plaintiffs assert against breached companies in the wake of a data breach, whether they be contractual, tortious, statutory, or equitable, is the essential element of cognizable injury.[9] With very few exceptions, a plaintiff must show that he or she suffered some appreciable, non-speculative, present harm to state a claim for relief.[10] So far, no element has proven more elusive for plaintiffs.[11] As explained below, absent allegations of actual, detrimental misuse of their information, plaintiffs have had great difficulty establishing any injury sufficient to support their claims.

Increased Risk of Future Harm: The most commonly alleged injury in data breach actions is an increased risk of future harm. Specifically, consumers frequently have alleged that as a result of the exposure of their information,

[9] *See, e.g., Shafran v. Harley-Davidson, Inc.*, No. 07 CIV. 01365 (GBD), 2008 WL 763177, at *2-3 (S.D.N.Y. Mar. 20, 2008).
[10] *See, e.g., Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010).
[11] As we explain below in the section on procedural issues, this lack of injury also often prevents plaintiffs who sue in federal court from meeting the requirements for standing under Article III of the US Constitution.

they are now at risk of having that information misused to commit future instances of identity theft, fraud, or phishing. Courts have routinely held that this is insufficient to state a claim.[12]

Time and Money Spent Mitigating Risk of Future Harm: Closely related to allegations of a risk of future harm are allegations that plaintiffs expended time or money to mitigate that risk. For example, consumers frequently have alleged harm from the purchase of credit monitoring or identity theft insurance products. However courts have overwhelmingly rejected this theory of injury, finding that such mitigation costs are merely derivative of the speculative risk of future identity theft.[13] A notable outlier is *Anderson v. Hannaford Brothers*, in which an appeals court reversed the dismissal of the plaintiffs' claims under Maine law on the ground that credit monitoring and identity theft insurance products were reasonably foreseeable damages recoverable in negligence.[14] However, *Anderson*'s applicability is likely limited to its very unique facts, as plaintiffs there claimed widespread and ongoing fraud that the defendant conceded was the result of a breach of its systems.[15]

Emotional Injury and Loss of Privacy: Plaintiffs have similarly alleged that the exposure of their information injured them by causing emotional injury, such as anxiety or stress, or a loss of privacy. Neither theory appears to have been embraced by courts. Courts have generally found allegations of emotional distress to be insufficient to state a claim for relief.[16] As to loss of privacy, some courts have held that a loss of privacy constitutes actionable

---

[12] *See, e.g.*, *Grigsby v. Valve Corp.*, C12–0553JLR , 2012 WL 5993755, at *2 (W.D. Wash. Nov. 14, 2012); *Shafran*, 2008 WL 763177, at *2-3; *see also Krottner*, 406 F. App'x at 131; *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 635, 640 (7th Cir. 2007).

[13] *See Grigsby*, 2012 WL 5993755, at *2; *see also Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913-6 (N.D. Cal. 2009), *aff'd*, 380 F. App'x 689, 691-92 (9th Cir. 2010); *Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc.*, CIV.A 08-1568, 2009 WL 799760, at *4-5 (E.D. La. Mar. 24, 2009); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 284 (S.D.N.Y. 2008).

[14] *Anderson*, 659 F.3d at 162–67.

[15] *Id.* at 164 (1st Cir. 2011). As explained below, mitigation damages of the sort sustained in *Hannaford* also are likely not recoverable in federal court under the Supreme Court's recent ruling in *Clapper v. Amnesty Int'l USA*, because "[plaintiffs cannot manufacture [Article III] standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 133 S. Ct. 1138, 1151 (2013).

[16] *See, e.g.*, *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 132-3 (D. Me. 2009), *aff'd in part, and rev'd in part sub nom. Anderson v. Hannaford Bros Co.*, 659 F.3d 151 (1st Cir. 2011).

harm only if there is an intentional or egregious invasion of privacy not present in actions against breached companies,[17] while others have rejected such claims of harm outright.[18]

Loss of Value of Information: Creative plaintiffs have also attempted to claim that the information they provided to the breached company had some ascertainable economic value, which was diminished by its exposure in the data breach. Courts, however, have consistently rejected the core concept of the theory—that consumer information has any economic value for which a consumer can expect to be compensated.[19] Apart from this defect, courts also have noted that plaintiffs tend to have difficulty demonstrating that a data breach caused any actual diminution in the alleged value of their information.[20] While one decision, *Claridge v. RockYou, Inc.*, allowed a negligence claim to survive a motion to dismiss based on a claim of "los[s] of the value of [information],"[21] it is unlikely to have any persuasive weight at this time. The court stated that the decision was motivated by the "paucity of controlling authority" at that time,[22] and declined to follow it in subsequent cases.[23]

Benefit of the Bargain: Recently, plaintiffs have also claimed injury by alleging that they did not receive the benefit of the bargain with respect to a purchase from the defendants. This theory has met little success thus far. For example, the plaintiffs in *Barnes & Noble* and *In re LinkedIn User Privacy Litig.* each alleged that they paid a premium for the items they purchased from the defendants that was allocated to security of their information.[24] In

---

[17] *See, e.g.*, *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 711 (D.C. 2009); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008).

[18] *Hammond v. The Bank of New York Mellon Corp.*, 08 CIV 6060 RMB RLE, 2010 WL 2643307, at *7–8, *11 (S.D.N.Y. June 25, 2010); *Willey v. J.P. Morgan Chase, N.A.*, 09 CIV 1397(CM), 2009 WL 1938987, at *10 (S.D.N.Y. July 7, 2009).

[19] *In re Barnes & Noble Pin Pad Litig.*, 12-CV-8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013); *In re Jetblue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 326-7 (E.D.N.Y. 2005).

[20] *LaCourt v. Specific Media, Inc.*, SACV 10-1256-GW JCGX, 2011 WL 1661532, at *4-5 (C.D. Cal. Apr. 28, 2011).

[21] 785 F. Supp. 2d 855, 861, 866 (N.D. Cal. 2011).

[22] *Id.* at 861.

[23] *In re Facebook Privacy Litig.*, C 10-02389 JW, 2011 WL 6176208, at *5 (N.D. Cal. Nov. 22, 2011).

[24] *Barnes & Noble*, 2013 WL 4759588, at *5; *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1092 (N.D. Cal. 2013).

each of these cases, the courts dismissed the plaintiffs' claim based on the benefit of the bargain theory as illusory, since the plaintiffs did not allege any defect with the product or service itself, nor any bargain with the defendant for a particular level of security.[25] By comparison, one recent decision denied a motion to dismiss based on the claimed loss of value of computer games sold by the defendant where the plaintiff specifically identified statements in which the defendant allegedly "assured" the plaintiffs that their information would be secure.[26]

Unreimbursed Losses: In contrast to the other theories discussed, plaintiffs are typically able to overcome the injury hurdle if they allege actual misuse of their information resulting in an unreimbursed monetary loss. Consumers who allege having to pay fraudulent charges on their payment cards have been found to satisfy the injury requirement.[27] Significantly, the plaintiff must actually incur the loss that is claimed. For example, it is well-established that a consumer has not suffered any cognizable injury related to a fraudulent credit card charge if that charge was later reimbursed by the card issuer, as often occurs.[28] Further, if an instance of identity theft fails to result in any actual loss to the consumer, there has been no recoverable injury.[29]

Causation of Damages

Apart from the requirement to show cognizable injury, plaintiffs typically must show that the claimed injury was caused by the defendant's actions. In data breach cases, causation is a particularly prominent issue with respect to allegations of actual misuse of a plaintiff's information. A central question with which the court must grapple is what allegations—and later, evidence—is required to show that a particular instance of misuse was perpetrated using data stolen from the breached company. In *Slaughter v. AON Consulting, Inc.*, the court crystallized this issue by dismissing claims for negligence under Delaware law, because the plaintiffs had not provided any reason to believe that the two claimed instances of identity theft "were not the result of

[25] *Id.*
[26] *Grigsby v. Valve Corp.*, 12-CV-00553, slip op. at *8 (W.D. Wash. Mar. 18, 2013).
[27] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 527 (N.D. Ill. 2011).
[28] *Anderson*, 659 F.3d at 155 n.2 (1st Cir. 2011); *In re Michaels Stores*, 830 F. Supp. 2d at 527.
[29] *Krottner*, 406 F. App'x at 131.

something else."[30] By contrast, the Ninth Circuit in *Stollenwerk v. Tri-West Health Care Alliance* found a showing of detailed factual information to support temporal and logical connections between the breach and misuse to be sufficient, in that case, to avoid dismissal at summary judgment.[31] The inability to plead reliance on assurances of security has also been the focus of some cases dismissing for lack of causation.[32]

Limitations under Particular Causes of Action

Finally, damages that would otherwise be recoverable may be prohibited because of principles that are specific to the cause of action the plaintiff is bringing. For instance, defendants in data breach actions often seek dismissal of negligence claims based on the economic loss doctrine.[33] In general, the economic loss doctrine forecloses a purchaser of a product or service from recovering in tort for economic losses without accompanying damage to person or property, and instead requires that any action be brought on a contract theory, if at all.[34] Defendants in data breach cases have achieved success in obtaining dismissal of negligence claims based on the economic loss doctrine under various states' laws.[35] Courts have rejected attempts to argue that the exposure of electronic data, or the destruction (by the plaintiffs) of their credit cards to prevent further fraud, amounted to "property damage" precluding the application of the economic loss doctrine.[36] However, the contours of the economic loss doctrine can vary from state to state, and certain states impose at least some limitations on its application. Given these nuances, data breach defendants have not been uniformly successful in asserting the economic loss doctrine to defeat negligence claims at the motion to dismiss stage.[37]

---

[30] *Slaughter v. AON Consulting, Inc.*, CIV.A. 10C-09-001FSS, 2012 WL 1415772, at *2, *4 (Del. Super. Jan. 31, 2012).

[31] *Stollenwerk v. Tri-W. Health Care Alliance*, 254 F. App'x 664, 668 (9th Cir. 2007) (reversing summary judgment); *see also Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1325-9 (11th Cir. 2012).

[32] *In re LinkedIn*, 932 F. Supp. 2d at 1092.

[33] *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 918 N.E.2d 36, 46-7 (Mass. 2009).

[34] *Apollo Grp., Inc. v. Avnet, Inc.*, 58 F.3d 477, 480-1 (9th Cir. 1995).

[35] *Cumis*, 918 N.E.2d at 46-7 (holding that Massachusetts law precluded recovery in negligence for economic loss in a data breach case); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 175-78 (3d Cir. 2008) (same result under Pennsylvania law).

[36] *In re TJX*, 564 F.3d at 498; *Cumis*, 918 N.E.2d at 46-7.

[37] *See Lone Star Nat'l Bank supra* n. 5; *Merrick Bank Corp.*, 2008 WL 4277877, at *7-8.

Causes of Action Asserted

Even if data security breach plaintiffs allege a sufficient injury causally connected to the defendant's conduct, they must still assert the remaining elements of a valid cause of action. We explain below the claims that are often asserted, as well as how courts have addressed them.

Contract

Plaintiffs frequently assert contract-based theories in data security breach litigation. A plaintiff pressing a breach-of-contract claim must plead and prove:

1. the existence of a binding contract or agreement;
2. the non-breaching party fulfilled its contractual obligations;
3. the breaching party failed to fulfill its contractual obligations without legal excuse; and
4. the non-breaching party suffered damages as a result of the breach.[38]

Plaintiffs in data security cases often claim that the breached company made a contractual promise to protect personal information and breached that obligation.

Setting aside the above-described difficulties involved in showing both the fact and the causation of damages, claimants have in many instances stumbled on the threshold requirement of showing a binding promise by the breached company. For instance, many courts have declined to treat a company's statements about its security practices, such as in a privacy policy, as an enforceable contract.[39] Where a payment card brand claims that a merchant or its acquiring bank agreed to pay fines and assessments for compromising payment card data, one court has suggested that such promises are unenforceable under state law because they are contractual penalties.[40]

In many instances, plaintiffs have sought to address the absence of an express agreement by claiming that the breached company created an "implied"

[38] *Rachells v. Cingular Wireless*, 483 F. Supp. 2d 583, 589 (N.D. Ohio 2007).
[39] *See, e.g., In re Zappos.com, Inc.*, 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013); *but see Jetblue Airways*, 379 F. Supp. 2d at 325-26 (treating privacy policy as contract for purposes of motion to dismiss).
[40] *Genesco*, 2013 WL 3790647, at *23.

contract to safeguard data when it collected their personal information. An implied contract typically requires all of the elements of an express contract, except that the parties' assent is manifested through conduct rather than words.[41] In limited circumstances some courts have sustained data security plaintiffs' claims, for purposes of a motion to dismiss, that a merchant from whom they purchased goods or services implicitly agreed to take reasonable measures to protect their information.[42] By contrast, at least one court has rejected such a claim.[43] Courts have routinely dismissed such claims against breached companies with whom the plaintiffs shared no direct relationship, on the ground that absent direct dealings, there is no basis to infer from the parties' conduct mutual asset to contract.[44]

Plaintiffs have also sought to address a lack of a direct relationship with the breached company by claiming they are "third party beneficiaries" of, and thus entitled to enforce, the company's contracts with other parties in which the company promised to safeguard personal information. These claims, however, require the plaintiffs to plead and prove that the contracting parties intended to benefit the plaintiffs through their contract, as opposed to merely conferring a benefit on the plaintiffs incidentally.[45]

Tort

Tort-based theories of liability in data security breach cases typically involve claims for negligence and/or negligent misrepresentation, but can occasionally give rise to other tort claims as well.

Negligence: As noted above, plaintiffs in data breach actions frequently assert negligence claims under the theory that the breached defendant had a duty to exercise reasonable care in protecting the plaintiffs' personal information, and that the defendant breached that duty by failing to establish adequate

[41] *In re Heartland Payment Sys., Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566, 581 (S.D. Tex. 2011), *rev'd in part sub nom. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421 (5th Cir. 2013).
[42] *See, e.g., In re Hannaford Bros.*, 613 F. Supp.2d at 119.
[43] *In re Zappos.com*, 2013 WL 4830497, at *3.
[44] *See, e.g., Willingham v. Global Payments, Inc.*, 1:12-CV-01157-RWS, 2013 WL 440702, at *18 (N.D. Ga. Feb. 5, 2013) (recommending dismissal where consumers and payment processor had no direct relationship).
[45] *Id.* at *20 (recommending dismissal of a claim by consumers that they were third party beneficiaries of a payment processor's contracts with merchants).

safeguards to protect the information and/or by failing to provide timely notification of the breach.[46] To succeed on a negligence claim, plaintiffs typically must show:

1. the existence of a duty to exercise due care,
2. breach of that duty,
3. causation, and
4. damages.[47]

In addition to facing difficulties associated with showing cognizable injury and causation, and with overcoming the economic loss doctrine (as noted above), plaintiffs must also plead and prove the threshold requirement that the defendant owed them a duty of care.[48] Courts have been particularly likely to reject plaintiffs' efforts to meet this requirement where, for example, the plaintiffs and the defendant have no direct relationship,[49] or where the posited duty derives from a statute that does not apply to the facts of the case.[50]

Negligent and/or Intentional Misrepresentation: In addition to negligence claims, plaintiffs in data breach actions frequently assert claims for misrepresentation, claiming that the defendant, whether in its advertising, marketing, privacy policies, or bank contracts, represented that it would take reasonable measures to safeguard customer information.[51] To state a claim for negligent misrepresentation, a plaintiff must allege:

1. that the defendant made a material misrepresentation;
2. with negligence, i.e., without reasonable ground for believing it to be true;
3. that the plaintiff justifiably relied on the statement; and
4. that, as a result of this reliance, the plaintiff suffered injury.[52]

---

[46] *See, e.g.*, *Ruiz v. Gap, Inc.*, 380 F. App'x. 689, 691; *TJX*, 564 F.3d at 498-99.
[47] *Ruiz*, 380 F. App'x. at 691.
[48] *Merrick Bank Corp.*, 2008 WL 4277877, at *11-12 (dismissing negligence claim in data security breach suit for lack of duty).
[49] *Willingham*, 2013 WL 440702, at *18 (a breached payment processor owed no duty to consumers who provided information to third party merchants).
[50] *Id.* (no duty under a statute requiring provision of notice of breach to Georgia residents, where the plaintiffs were not Georgia residents).
[51] *In re TJX*, 564 F.3d at 494.
[52] *Small v. Fritz Companies, Inc.*, 65 P.3d 1255, 1258 (Cal. 2003).

A claim of intentional or fraudulent misrepresentation has similar elements, with a heightened scienter requirement.[53] In addition to prevailing on the damages issues described above, defendants in data breach matters have also succeeded in pressing arguments that plaintiffs failed to demonstrate reasonable or "justifiable" reliance on the alleged misstatement made by the defendant.[54]

Other Tort-Based Theories: Plaintiffs will occasionally proffer other tort-based theories of liability, such as negligence per se, conversion, breach of fiduciary duty, or tortious interference, which have met little success.

Other Common Law Principles

Unjust Enrichment: Unjust enrichment is a quasi-contractual theory of recovery that private litigants have asserted in several recent data breach actions.[55] Although the elements of a claim for unjust enrichment vary by state, a plaintiff must typically at least allege that he or she conferred a benefit on the defendant, the retention of which is unjust.[56] Since a benefit is required, claims for unjust enrichment are ordinarily brought only by data breach plaintiffs who allege having purchased some product or service from the defendant.[57]

Although unjust enrichment provides plaintiffs with an alternative to traditional contract and tort actions, it has its own obstacles that plaintiffs have found difficult to overcome. As a threshold matter, not all states

---

[53] *Id*.

[54] *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club*, 455 Mass. 458, 471-6 (2009) (affirming summary judgment for defendant because credit unions could not have reasonably relied on any alleged misrepresentations); *see also In re Heartland Payment Sys*., 834 F. Supp. 2d at 594 (dismissing negligent misrepresentation claim under Rule 12(b)(6) because allegation of reliance was conclusory), *rev'd in part sub nom. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421 (5th Cir. 2013).

[55] While this section explores courts' treatment of claims for unjust enrichment, the principles discussed are likely applicable to similar equitable claims, such as restitution or money had and received.

[56] *See, e.g., AMP Servs. Ltd. v. Walanpatrias Found.*, 73 So. 3d 346, 350 (Fla. Dist. Ct. App. 2011); *Hertz Corp. v. RAKS Hospitality, Inc.*, 196 S.W.3d 536, 543 (Mo. Ct. App. 2006); *Martin v. E. Lansing Sch. Dist.*, 483 N.W.2d 656, 661 (Mich. Ct. App. 1992); *R. Zoppo Co., Inc. v. City of Manchester*, 453 A.2d 1311, 1313 (N.H. 1982).

[57] *See, e.g., Bell v. Blizzard Entm't, Inc.*, No. 12-CV-09475 BRO (PJWx), slip op. at *7-8 (C.D. Cal. July 11, 2013) (consumers alleged that a video game developer sold them games, but failed to abide by assurances in its privacy policy).

recognize unjust enrichment as a standalone cause of action.[58] Even where unjust enrichment provides a standalone cause of action under state law, it is often unavailable where the plaintiff has an adequate remedy at law or where there is an express contract between the parties that governs the dispute.[59]

Bailment: A more novel claim asserted by plaintiffs in recent years is that the defendant is liable for a data breach as the bailee of plaintiffs' information. Bailment is the relationship that arises when personal property is delivered to another for some particular purpose with an express or implied contract to redeliver the property when the purpose has been fulfilled, or to otherwise deal with the property according to the bailor's instructions.[60] A classic example of bailment is the delivery of a car to a parking attendant.[61]

Though creative, claims for bailment in the data security space have not proven to be viable.[62] For one thing, no court has accepted the proposition that consumer information is "property" of a type that can be bailed.[63] For another, as courts have noted, it is unclear how such information can be "delivered" to companies or "returned" to consumers.[64] Moreover, courts have noted that in the typical data breach action, there is no allegation that the defendant was involved in perpetrating the theft, or that the defendant otherwise sought to deprive plaintiffs of their information.[65] Accordingly, bailment is not a claim likely to benefit most plaintiffs.

State Statutes

In addition to common law claims, data breach plaintiffs frequently assert causes of action under state consumer protection statutes. State by state

---

[58] *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 973-4 (S.D. Cal. 2012) (dismissing an unjust enrichment claim under California law in a data breach case for this reason).
[59] *See, e.g.*, *Bell supra* n. 57 at *8 (citing *BAE Sys. Info. & Elec. Sys. Integration v. Lockheed Martin Corp.*, CIV.A. 3099-VCN, 2009 WL 264088, at *7 (Del. Ch. Feb. 3, 2009)).
[60] *Earhart v. Callan*, 221 F.2d 160, 163 (9th Cir. 1955).
[61] *See* BLACK'S LAW DICTIONARY (9th ed. 2009).
[62] *In re Sony Gaming Networks*, 903 F. Supp. 2d at 974-5; *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1126-7 (N.D. Cal. 2008), *aff'd*, 380 F. App'x 689 (9th Cir. 2010); *Richardson v. DSW, Inc.*, 05 C 4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005); *Bell*, No. 12-CV-09475, at *15-16.
[63] *See Bell*, No. 12-CV-09475, at *15.
[64] *In re Sony Gaming Networks*, 903 F. Supp. 2d at 974.
[65] *Id.*; *Ruiz*, 540 F. Supp. 2d at 1127.

variations in the requirements under these statutes can exist, but they often proscribe deceptive and/or unfair business practices. Some states also have data breach notification statutes that allow a cause of action for injury flowing from a breach of the statute's requirements. Courts have held data breach plaintiffs proceeding under an "unfairness" theory to a high standard of proof. Specifically, a plaintiff must show that the data security practices were (1) "systematically reckless," (2) "aggravated by [a] failure to give prompt notice," and (3) "cause[d] very widespread and serious harm to…innumerable consumers."[66] Furthermore, courts in data security breach cases have held that certain consumer protection statutes are intended to protect consumers, and thus commercial entities such as issuing banks are not proper plaintiffs under these statutes.[67]

Federal Statutes

Fair Credit Reporting Act: Private litigants have also brought claims against companies that suffer data security breaches pursuant to the Fair Credit Reporting Act (FCRA),[68] but a number of courts have dismissed such claims at the pleading stage.

The Fair Credit Reporting Act creates obligations on three types of parties: (1) consumer reporting agencies,[69] (2) furnishers of credit information to consumer credit reporting agencies,[70] and (3) users of consumer credit reports.[71] Recent data security breach cases have tended to involve claims relating to the FCRA's provisions governing consumer reporting agencies. Such claims frequently involve two threshold issues: (1) whether the company that was subject to the data security breach falls under the definition of a consumer reporting agency, and (2) whether the company violated the FCRA's requirement that such an agency establish "reasonable procedures designed to…limit the furnishing of consumer reports to the purposes" permitted by the statute.[72] Plaintiffs have faced an uphill battle

[66] *See In re Michaels Stores*, 830 F. Supp. 2d 518, 526 (N.D. Ill. 2011) (citing *In re TJX*, 564 F.3d at 496).
[67] *See, e.g., In re Heartland Payment Sys.*, 834 F. Supp. 2d at 605-07.
[68] 15 U.S.C. §§ 1681 *et seq*. (West).
[69] 15 U.S.C. § 1681e.
[70] 15 U.S.C. § 1681s-2.
[71] 15 U.S.C. § 1681m.
[72] *See* 15 U.S.C § 1681e(a).

characterizing a breached company as a "consumer reporting agency" subject to the statute, which courts have typically limited to those entities traditionally understood to be the three major credit reporting bureaus—Experian, Equifax, and TransUnion.[73] Other courts have grounded their dismissals on the plaintiffs' failure to demonstrate that the defendant creates "consumer reports" as opposed to merely handling payment or other consumer information.[74] Courts have also rejected plaintiffs' arguments that the plaintiffs' data was "furnished" for purposes of the statute, holding that allegations of theft cannot be construed as "furnishing" a consumer report.[75]

Other Federal Statutes: In addition, data breach plaintiffs occasionally bring actions under other federal statutes, including sections of the Electronic Communications Privacy Act (ECPA),[76] commonly referred to as the Wiretap Act. Although actual damages are not required to state a claim under certain provisions of the Wiretap Act,[77] actions under this provision are brought infrequently because, to state a claim, a plaintiff must allege that the defendant engaged in the intentional interception, disclosure, or use of data or communications in violation of the Wiretap Act.[78] Similarly, data breach plaintiffs occasionally assert claims for violation of the Stored Communications Act (SCA),[79] the section of the ECPA barring providers of certain communication services from divulging private communications to third parties; however, such claims have also been unsuccessful to date.[80]

Data security-related suits by shareholders under securities statutes have likewise been infrequent, because such shareholders face difficulty pleading

---

[73] *See, e.g., Holmes v. Countrywide Fin. Corp.*, 5:08-CV-00205-R, 2012 WL 2873892, at *15 (W.D. Ky. July 12, 2012); *F.T.C. v. Gill*, 265 F.3d 944, 948 (9th Cir. 2001).
[74] *Fuges v. Sw. Fin. Servs., Ltd.*, 707 F.3d 241, 252-5 (3d Cir. 2012); *Willingham*, 2013 WL 440702, at *13-14 (Mag. Judge's Final Report and Recommendation); *Garnett v. Millennium Med. Mgmt. Res., Inc.*, 10 C 3317, 2010 WL 5140055, at *2-3 (N.D. Ill. Dec. 9, 2010).
[75] *Holmes*, 2012 WL 2873892, at *16.
[76] 18 U.S.C. §§ 2510–22 (West).
[77] *See* 18 U.S.C. § 2520(c)(2).
[78] *See* 18 U.S.C. §§ 2511(1)(a), (c) & (d).
[79] 18 U.S.C. §§ 2701–11 (West).
[80] *See, e.g., In re Michaels Stores*, 830 F. Supp. 2d at 523-5 (holding that the craft retailer did not provide "electronic communication services" or "remote computing services," as necessary to state a claim under the SCA).

and proving that the breached company made material misstatements or omissions about its security practices, that it did so with the requisite scienter, and that the alleged misrepresentations or omissions caused losses to the shareholders.[81]

Procedural Issues

Article III Standing

Data breach plaintiffs seeking to invoke federal jurisdiction must satisfy the standing requirements of Article III of the United States Constitution. Specifically, a plaintiff must show an injury-in-fact that is "(a) concrete and particularized" and "(b) actual or imminent, not conjectural or hypothetical."[82] Further, plaintiffs must demonstrate that the claimed injury is fairly traceable to the conduct complained of.[83]

Constitutional standing has emerged as a prominent issue in the data security space, as it addresses the core issue in the practice discussed above: whether plaintiffs have suffered any actual injury as a result of the breach. In the rare instance where plaintiffs claim actual misuse of the information compromised in the breach, there is little doubt that plaintiffs satisfy Article III's injury-in-fact requirement.[84] Conversely, courts agree that plaintiffs fall short of establishing any injury-in-fact where they cannot show that their information was compromised.[85] Where plaintiffs' allegations of injury fall between these two extremes—such as where plaintiffs claim harm from the mere exposure of their information during a data breach—the courts have split.[86]

---

[81] *See In re Heartland Payment Sys. Inc. Sec. Litig*., CIV. 09-01043, 2009 WL 4798148, at *3-8 (D. N.J. Dec. 7, 2009) (dismissing a shareholder federal securities suit because the plaintiffs failed to plead material misstatements and scienter); *In re Choicepoint, Inc. Sec. Litig.*, No. 05-00686, slip op. at 6-9 (N.D. Ga. July 21, 2008) (despite having initially denied the defendant's motion to dismiss, approving settlement in part because of a significant risk that the plaintiffs would fail to prove material misstatements or omissions, scienter, and loss causation).

[82] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal citations omitted).

[83] *Id*.

[84] *See, e.g.*, *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008).

[85] *Katz v. Pershing, LLC*, 672 F.3d 64, 79 (1st Cir. 2012); *Hammer v. Sam's East, Inc.*, 12-CV-2618-CM, 2013 WL 3756573, at *3 (D. Kan. July 16, 2013).

[86] *Compare, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011) (no standing), *with Pisciotta*, 499 F.3d at 634 (standing satisfied).

However, a recent decision by the United States Supreme Court appears to have resolved this split in favor of the courts finding a lack of standing. In *Clapper v. Amnesty International USA*, the Supreme Court dismissed for lack of standing a suit brought by attorneys and organizers who alleged that their communications were likely to be monitored under a purportedly unconstitutional federal surveillance statute, given that they worked with persons likely to be targeted for surveillance.[87] Although the dispute in *Clapper* did not involve a data breach, the decision's potential implications for the data security space are clear. For one, the Court expressly rejected the proposition that an "objectively reasonable likelihood" of harm can suffice for standing, instead holding that the threatened harm must be "certainly impending."[88] Further, the Court's rejection of standing based on a "speculative chain of possibilities" in *Clapper* is closely analogous to the Third Circuit's reasoning in *Reilly* that speculation as to a hacker's intent or ability to commit identity theft does not create standing.[89] Finally, two federal district courts have already applied the *Clapper* decision in the data breach context, in each case dismissing the plaintiffs' complaint for lack of standing.[90] Accordingly, although the full weight of the Supreme Court's decision in *Clapper* has yet to be felt, it appears that the door to the federal courthouse may be closing for plaintiffs who are unable to allege actual misuse of their information.

Federal courts hearing data security breach cases have also been largely unreceptive to other theories of standing. For example, plaintiffs have claimed harm from time and money spent mitigating the purported risk of identity theft, such as for credit monitoring services. However, the Supreme Court's decision in *Clapper* appears to have foreclosed that theory as well.[91] Plaintiffs have also asserted injury from a purported diminution in the economic value of their information, but numerous courts have dismissed such claims on Article III standing grounds.[92] With

---

[87] *Clapper*, 133 S. Ct. at 1148-50.
[88] *Id.* at 1143.
[89] *Compare Clapper*, 133 S. Ct. at 1148-50 *with Reilly*, 664 F.3d at 45.
[90] *See Barnes & Noble*, 2013 WL 4759588, at *5 (speculation as to the risk of identity theft is insufficient under *Clapper*); *Hammer*, 2013 WL 3756573, at *2-3.
[91] *See Barnes & Noble*, 2013 WL 4759588, at *4; *Clapper*, 113 S. Ct. at 1151 ("[Plaintiffs] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").
[92] *Barnes & Noble*, 2013 WL 4759588, at *5; *In re iPhone App. Litig.*, No. 11-02250, 2011 WL 4403963, *4-5 (N.D. Cal. Sept. 20, 2011); *LaCourt v. Specific Media, Inc.*, No. 10-1256,

respect to claims of generalized anxiety or stress, courts in particular contexts have reached differing conclusions as to whether such injuries are sufficient to confer standing,[93] but *Clapper* suggests that such theories will be rejected going forward.[94] Finally, plaintiffs have also had mixed results in alleging injury-in-fact from their failure to receive the benefit of the bargain.[95] Where the claim is misrepresentation-based, however, this theory has been held not to suffice to establish standing absent an allegation that the plaintiffs actually read the purported misrepresentations regarding the defendant's security practices.[96]

Class Certification

Plaintiffs in data security breach cases often seek to bring litigation as a class action. However, such plaintiffs face significant challenges in obtaining certification of a class. When seeking certification in federal court under Federal Rule of Civil Procedure 23, the burden is on the representative plaintiffs to show that the prerequisites of Rule 23(a)—numerosity, commonality, typicality, and adequacy—are satisfied. In addition, the representative plaintiffs must provide evidentiary proof that "questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy."[97] As clarified by the Supreme Court in 2011, this is more than a "mere pleading standard."[98] In fact, trial courts addressing the issue are instructed to conduct a "rigorous analysis."[99] As a result, courts frequently deny class certification in data breach litigation.

In particular, even where data security breach plaintiffs are able to satisfy the requirements of Rule 23(a), Rule 23(b) has proven to be a significant obstacle

---

2011 WL 2473399, at *4-5 (C.D. Cal. Apr. 28, 2011); *but see also Claridge*, 785 F. Supp. 2d at 861.

[93] *Compare Krottner*, 628 F.3d at 1142 (sufficient), *with Reilly*, 664 F.3d at 44-45 (insufficient).

[94] *Clapper*, 113 S. Ct. at 1151.

[95] *Compare Grigsby*, No. 12-CV-00553, slip op. at *8 (allowing standing) *with Barnes & Noble*, 2013 WL 4759588, at *5 (denying standing) *and In re LinkedIn*, 2013 WL 844291, *4 (same).

[96] *In re LinkedIn*, 2013 WL 844291, at *4.

[97] *See* FED. R. CIV. P. 23(b)(3).

[98] *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011).

[99] *Id*.

to class certification.[100] Rule 23(b)(3) permits class certification only if "the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members."[101] However, data breach litigation claims are often based on individual issues of causation and damages. To establish misrepresentation, for instance, plaintiffs must prove reliance on an inaccurate representation (or omission). Even when uniform misrepresentations are made to potential class members, the plaintiffs' reactions to the defendant's misrepresentation could, and likely will, differ. As one court explained, proving reliance "will necessarily involve individual questions of fact."[102] In data breach litigation particularly, there is a strong argument that some plaintiffs did not rely on the alleged misrepresentation when deciding to provide personal information.

Similarly, plaintiffs have a difficult time arguing that fraud losses are consistent across the class. In a recent data security breach case decided on the issue of predominance, *In re Hannaford Bros. Co. Customer Data Sec. Breach Litigation*, customers' credit and debit card information was stolen from a grocery store.[103] The court noted that questions relating to the company's conduct were common to the class, but the actual impact of the data breach varied from plaintiff to plaintiff: "where things differ is in the actual impact on particular cardholders…and the actual mitigating steps they took and the costs they incurred."[104] The court ultimately denied certification because the plaintiffs had not presented any expert testimony demonstrating that total damages incurred by the putative class could be proven by statistical methods.[105] Likewise, *In re TJX* ruled that the predominance requirement was not met because losses that result from or are related to fraudulent transactions could not be demonstrated on a classwide basis, "[g]iven that there are a myriad of ways in which fraud losses can occur, as well as the fact that the plaintiffs themselves have admitted the difficulty of attributing any particular loss to the data breach."[106]

---

[100] A class may also be certified if it meets any of the three requirements of 23(b). However, b(1) and b(2) classes rarely arise in data breach litigation and are therefore not addressed in this chapter.
[101] FED. R. CIV. P. 23(b)(3).
[102] *In re TJX Cos. Retail Sec. Breach Litig.*, 246 F.R.D 389, 395 (D. Mass. 2007).
[103] *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 2:08-MD-1954-DBH, 2013 WL 1182733, *1 (D. Me. Mar. 20, 2013).
[104] *Id*. at *8.
[105] *Id*. at *9-10.
[106] *In re TJX Companies*, 246 F.R.D. at 397.

Claims for Indemnification by the Breached Company

While thus far we have focused on claims against a corporate victim of a data security breach, it also bears noting that such a company is not necessarily without recourse to recoup losses it suffers by reason of the breach. Such companies sometimes seek indemnification from third parties, such as from service providers or technology suppliers that allegedly were at fault for the breach, or insurers that allegedly issued policies covering the losses resulting from the breach.

Few such suits have drawn judicial opinions, but those that have suggest that at least some viable claims can be pressed by breach victims. A recent decision permitted a suit against a provider of technology and related services to proceed to trial in federal court.[107] There, restaurant chain Cotton Patch Cafe (Cotton Patch) sued payment processing equipment provider Micros Systems, Inc. (Micros) over alleged deficiencies in a Micros payment processing system that purportedly caused a payment card data breach at one of Cotton Patch's restaurants in Nacogdoches, Texas, requiring the restaurant to pay over $250,000 in fines and assessments imposed by Visa and MasterCard.[108] Cotton Patch sued Micros for damages in the US District Court for the District of Maryland, asserting claims for violation of Texas's Deceptive Trade Practices Act, negligence, negligent misrepresentation, gross negligence, and fraud by nondisclosure.[109] The court granted summary judgment to Micros on Cotton Patch's claims for negligence and gross negligence under Texas law based on the economic loss doctrine, but denied Micros's motion for summary judgment on the restaurant's claims under the Deceptive Trade Practices Act and for negligent misrepresentation and fraud by nondisclosure.[110] As to the misrepresentation and fraud claims, the court reasoned that there were genuine issues of material fact as to whether Micros misrepresented or withheld information regarding security deficiencies in the payment processing system.[111] On the Deceptive Trade Practices Act claim, the court reasoned that there were

[107] *Cotton Patch Cafe, Inc. v. Micros Sys., Inc.*, CIV.A. MJG-09-03242, 2012 WL 5986773 (D. Md. Nov. 27, 2012).
[108] *Id*. at *2.
[109] *Id*. at *3.
[110] *Id*. at *9.
[111] *Id*. at *7-8.

genuine issues of material fact as to whether Cotton Patch was a "consumer" entitled to protection under the statute.[112] The parties tried the case before a jury for two days, and then settled the dispute and stipulated to a full dismissal.[113]

In addition, at least one decision has sustained a claim by a breached company against an insurer. Recently, the US Court of Appeals for the Sixth Circuit affirmed summary judgment in favor of a data security breach victim, DSW Shoe and certain related companies, against an insurer that contested coverage of losses DSW suffered from a data security breach in which hackers stole customer payment card information from the retailer's computer network.[114] DSW had "incurred expenses for customer communications, public relations, customer claims and lawsuits, and attorney fees" in connection with investigations by government agencies, as well as assessments imposed by the credit card brands.[115] The Sixth Circuit affirmed summary judgment for DSW on the ground that its losses were covered under an insurance policy that covered "[l]oss which the Insured shall sustain resulting directly from…[t]he theft of any Insured property by Computer Fraud."[116]

Conclusion

As the above discussion demonstrates, even accepting the prevailing wisdom that every company has or will at some point be victimized by a data breach, and must incur significant legal, customer relations, and other costs as a result, far from every such company will be held legally responsible to private litigants. Courts are often hesitant to open their doors to redress the types of intangible or speculative harm (if any) that such breaches frequently create, and in any event, a company's being victimized by a data security breach does not necessarily mean it has breached its legal obligations. As plaintiffs continue to press claims over data security breaches, practitioners in this area should closely watch for further developments in this continuously evolving area of the law.

---

[112] *Id*. at *8-9.
[113] Joint Stipulation of Dismissal with Prejudice (filed Sept. 4, 2013).
[114] *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F.3d 821 (6th Cir. 2012).
[115] *Id*. at 824.
[116] *Id*. at 827, 831-4.

Key Takeaways

- Make clients who have suffered a data security breach aware that they may face claims by a variety of private litigants, such as the individual or individuals whose data was potentially stolen or at risk of being stolen, issuing banks and payment card brands (if payment card data was potentially compromised), or shareholders.
- In defending private data security breach litigation, focus especially on issues surrounding lack of cognizable injury and damages to the plaintiff, as courts are often hesitant to open their doors to redress the types of intangible or speculative harm (if any) that data security breaches frequently create.
- Keep in mind that a company's being victimized by a data security breach does not necessarily mean it has breached its legal obligations.
- When advising a corporate victim of a data security breach, remind the client to review the potential for seeking indemnification from third parties, such as insurers.
- Watch for further developments in this continuously evolving area of the law to properly advise clients as plaintiffs continue to press claims over data security breaches.

Douglas H. Meal, a partner at Ropes & Gray LLP, represents companies in complex transaction-related disputes arising from all varieties of business agreements. Most recently, Mr. Meal has played a leading role in the firm's privacy and data security practice, specializing particularly in representing clients targeted by litigation and government investigations stemming from highly publicized data security breaches. As the lead outside lawyer handling claims stemming from the data security breaches suffered by Sony, Heartland Payment Systems, The TJX Companies, Nationwide, Hannaford Brothers, Aldo, Genesco, and Wyndham Hotels—some of the most highly publicized data security breaches in recent years—Mr. Meal has become the national leader in defending companies that suffer significant data security breaches involving consumer information against the ensuing claims and regulatory investigations.

Acknowledgment: *I thank my assistant author, associate David Cohen in Ropes & Gray LLP's Washington, DC office. Mr. Cohen, whose practice focuses on complex business and commercial disputes, has extensive experience working with corporate clients*

that have suffered data security breaches or have been accused of privacy violations, defending them against class actions and claims asserted by payment card brands, and representing them in connection with federal and state government investigations. I also thank the other Ropes & Gray LLP associates who contributed to the content and research for this chapter, including Sunil Shenoi, Lisa Rachlin, Dan Routh, and Joseph Cleemann.

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.

Each chapter in the *Inside the Minds* series offers thought leadership and expert analysis on an industry, profession, or topic, providing a future-oriented perspective and proven strategies for success. Each author has been selected based on their experience and C-Level standing within the business and legal communities. *Inside the Minds* was conceived to give a first-hand look into the leading minds of top business executives and lawyers worldwide, presenting an unprecedented collection of views on various industries and professions.

ASPATORE