Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell and Jason C Chipman

Second Edition

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2021
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at May 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-595-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON MORI & TOMOTSUNE

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

CRAVATH, SWAINE & MOORE LLP

RICHARD DENATALE

HUGHES HUBBARD & REED

K&L GATES LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its fifth edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Contents

Part II

Jurisdictional, Regional and Sectoral Nuances

10

US Litigation Considerations and Landscape

Kevin Angle, Richard Batchelder, Jr, Nameir Abbas, Danielle Bogaards, Anne Conroy, and Sara Ramsey[1]

Introduction

Almost inevitably, often within hours of the announcement of a data breach involving the personal information of any large number of individuals, plaintiffs start filing class action lawsuits seeking recovery for the incident. Even incidents potentially involving the personal information of a comparatively modest number of individuals can follow the same path.

This chapter canvasses the typical causes of action that plaintiffs assert in these cases in the United States and developing trends reflected in litigation regarding recent incidents.[2] The chapter also highlights key considerations in cybersecurity litigation that can drive strategy. Finally, the chapter reviews the latest case law as to the requisite 'injury' necessary for standing purposes following a data breach.

Typical causes of action in US litigation

Class action claims asserted in the data breach context typically fall into five broad categories: contract, negligence, other common law theories, US state unfair and deceptive practices statutes, and other federal or state statutes. In large incidents involving public companies, stock purchaser and shareholder derivative plaintiffs are also filing complaints with seemingly greater frequency.

Data breach theories of liability

Plaintiffs who bring claims arising from the potential exposure of personal information in a data breach typically allege lack of care, misrepresentation or lack of prompt notice. To

1 Kevin Angle is a counsel, Richard Batchelder, Jr is a partner and Nameir Abbas, Danielle Bogaards, Anne Conroy and Sara Ramsey are associates at Ropes & Gray LLP. The authors would like to recognise the work of Mark Szpak, a retired partner, who was a key contributor to the previous edition of this chapter.

2 US government enforcement actions are covered in Chapter 11 of this book.

survive a motion to dismiss, plaintiffs will need to show how their factual allegations state a claim for each theory advanced.[3]

Contract-based theories

Contract claims are common when there is a written agreement and contractual privity between the plaintiff (whose data was allegedly exposed) and the defendant (who incurred the breach), such as, for example, when the plaintiff has entered into a service contract with the defendant subject to written terms and conditions. If the written agreement contains an express contractual undertaking by the defendant to protect the security of the plaintiff's personally identifiable information (PII),[4] the contract claim is likely to turn on the specific language of the undertaking and how the defendant allegedly breached it.[5]

---

3 Apart from litigation brought on behalf of individuals whose personal data was allegedly exposed in an incident or shareholders in companies who incurred the breach, other types of litigation following such an incident (which are beyond the scope of this chapter) may include business-to-business lawsuits between the breached entity and service providers or business partners arising from disputes about responsibility for the incident or associated losses, or failure to maintain security as to the other party's data. For example, when retail businesses incur payment card breaches, complaints against the retailer have frequently been filed not only by cardholders claiming injury from the breach but also by financial institutions that may have issued the payment cards that were allegedly exposed, by which the financial institutions seek to obtain recovery from the retailer for claimed fraud losses following the breach or for costs allegedly stemming from replacing the cards, or both. See, e.g., *Community Bank of Trenton v. Schnuck Markets*, 887 F.3d 803, 807 (7th Cir 2018). Other types of litigation (also not addressed in this chapter) include disputes with insurers about cover.

4 Notably, a number of courts have held that a company privacy policy is not enforceable under a breach of contract theory when it is not expressly incorporated into a contract. See, e.g., *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 980 and 981 (ND Cal 2016) ('Plaintiffs can not bring a breach of contract claim . . . based on language from documents that might not even have been part of the alleged contract.'); *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.,* 19 N.Y.S. 3d 850, 860 (NY Sup Ct 2015) (finding plaintiffs failed to allege a contractual relationship with defendants despite privacy statement); *In re: Zappos.com, Inc.*, No. 2357, 2016 WL 2637810, at *6, n.3 (D Nev 6 May 2016) (finding that defendant's 'Safe Shopping Guarantee' language and lock-shaped icon on its website were unilateral statements and thus insufficient to show the existence of a contractual obligation). But see *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 484 (D. Md. 2020) (finding that privacy statements were objective offers to protect data security); *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir 2017) (finding that the privacy policy was incorporated in the relevant contract, but plaintiffs failed to allege a breach); *In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2017 WL 539578, at *11 (D Or 9 Feb 2017) (finding that complaint adequately alleged that defendant's privacy notice was (1) attached to and incorporated in the relevant contract, and (2) contained sufficient language to support the breach of contract claim).

5 See, e.g., *Scottrade*, 868 F.3d at 717 (dismissing contract claim based on defendant's privacy statement that 'we use [data] security measures that comply with federal law' in part because plaintiffs failed to identify an applicable law or regulation that defendant allegedly violated); *Dolmage v. Combined Ins. Co. of Am.,* No. 14 C 3809, 2015 WL 292947, at *7 (ND Ill 21 Jan 2015) (dismissing contract claim from initial complaint because plaintiff failed to allege facts demonstrating defendant breached its privacy pledge, which stated that it 'guard[s] [its customers'] personal information'). In cases where plaintiffs allege that a company's privacy policy can form an express contract, limitations within those policies may also block claims. See, e.g., *Pena v. British Airways, PLC (UK)*, No. 18-cv-6278 (LDH) (RML), 2020 WL 3989055, at *6 (EDNY 30 Mar 2020) (dismissing contract claim where 'Defendant's Privacy Policy explicitly states that it is "not contractual and d[oes] not form part of [plaintiff's] contract with [defendant]"') (internal citation omitted); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037 (ND Cal. 2019) (dismissing contract claims where Facebook's terms of service included an applicable limitation-of-liability clause); *In re Equifax, Inc.*, 362 F. Supp. 3d 1295, 1332 (ND Ga 2019) (rejecting claim

If a written agreement exists but has no written term as to the handling of personal data, or if there is no written agreement at all but the plaintiff is still in contractual privity with the defendant, the cause of action is typically styled as a breach of implied contract. Implied contract claims have received mixed treatment from courts. Some find that the typical purchase transaction does not include a promise to protect the PII that may have been obtained (e.g., payment card information in a retail purchase). In these cases, the courts hold that any implied contract, if it existed, 'involved only the provision of and payment for [the items in question], not a promise to safeguard the customer's [data]'.[6] Other courts accept that a defendant's receipt of consumer PII in connection with interactions of particular types can be sufficient to plead an implied contract covering the PII as well. These courts reason that 'it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently'.[7]

Finally, in cases without a written contract or privity between the parties, contract claims can be difficult to sustain. This situation commonly arises when the party receiving personal data from a plaintiff provides it to a third party for processing or handling, who suffers the breach. Absent direct dealings between the plaintiff (whose data was involved, albeit in the hands of a third party) and the third party (who incurred the breach), direct claims against the third party in contract tend to fail for inability to allege or show the requisite 'meeting of the minds'.[8]

---

where privacy policy stated defendant would not be liable for damages based on information found on the site). But see *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *45 (ND Cal 30 Aug 2017) (declining to dismiss contract claims where statements like using the service was 'AT YOUR OWN RISK' were contradicted by statements regarding security measures in place).

6 *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL, 2015 WL 4940371, at *3 (WD Wash 27 Mar 2015). See also *In re: SuperValu, Inc.*, 870 F.3d 763, 771 n.6 (8th Cir 2017) (rejecting breach of implied contract claim); *Longenecker-Wells v. Benecard Servs. Inc*, 658 F. App'x 659, 662 (3d Cir 2016) (same); *In re Equifax, Inc.,* 362 F. Supp. 3d at 1332 (same); but see *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 and 1177 (D Minn 2014).

7 *Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242, at *9 (ND Cal 14 Sep 2016). See also *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 750 and 751 (SDNY 2017) (denying motion to dismiss breach of implied contract claim); *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (ED Pa 2015) (same).

8 *Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060, 2010 WL 2643307, at *11 (SDNY 25 June 2010) (rejecting consumers' breach of implied contract claim on grounds that plaintiffs failed to allege direct dealings with defendant); *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *20 and *21 (ND Ga 5 Feb 2013) (rejecting consumers' breach of implied contract claim because plaintiffs provided their personally identifiable information [PII] to a merchant, not to the defendant). See also *Community Bank of Trenton v. Schnuck Markets*, 887 F.3d 803, 819 and 820 (7th Cir 2018) (rejecting implied contract claim brought by financial institution because 'the only business activity between the plaintiff banks and [defendant] happened (nearly instantaneously) through the indirect route of the card payment system, not in a direct face-to-face retail transaction'); *In re: Heartland Payment Sys., Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566 (SD Tex 2011), rev'd in part *sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir 2013) (same); but see *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 412 (ED Va 2020) (finding lack of privity did not bar unjust enrichment claim).

Negligence-based theories

Individuals alleging injury from the exposure of their personal information in a data breach almost always include a claim for negligence (i.e., that the breached entity acted negligently by failing to prevent the data from being accessed or acquired by an intruder). Of course, the merits of such claims, if litigated to a conclusion, often involve highly factual determinations and possibly expert testimony as to the adequacy of the defendant's security measures. However, cases rarely get that far.

The first question litigants must answer is whether the company had any duty to the plaintiff. The answer varies from state to state.[9] Courts in some cases have found no common law duty to safeguard personal information to exist under the law of the state in question.[10] At the same time, courts in other cases have concluded that a common law duty to safeguard personal information to have been sufficiently alleged, at least in certain factual contexts.[11]

Even when a duty of care is found to exist as a matter of law, the factual parameters of the standard for meeting that duty remain largely undefined. Though 'reasonableness' plays a prominent role in tort law generally, courts have not yet fully addressed how to determine 'reasonableness' in the data breach context.[12] Plaintiffs, for example, may frame the test as

---

9 Compare *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 478 (D Md 2020) (declining to find duty of care under Illinois law); *Dep't of Labor v. McConnell*, 828 S.E.2d 352, 358 (Ga 2019) (no duty to safeguard personal information under Georgia law); *Irwin v. Jimmy John's Franchise*, LLC, 175 F. Supp. 3d 1064, 1071 (CD Ill 2016) (no common law duty owed to customers under Arizona law), with *In re: Experian Data Breach Litig.*, No. SACV 15-1592 AG, 2016 WL 7973595, at *3, *5, *7 and *8 (CD Cal 29 Dec 2016) (denying motion to dismiss negligence claims brought by consumers under New York, Ohio, California or Illinois laws finding that plaintiff had alleged a duty under each state's law); *Hapka v. Carecentrix, Inc.*, No. 16-2372-CM, 2016 WL 7336407, at *5 (D Kan 19 Dec 2016) (denying motion to dismiss negligence claim brought by employees under Kansas law); *In re: Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1176 (D Minn 2014) (denying motion to dismiss negligence claims brought by customers under various state laws).

10 See, e.g., *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 17–18, 23–24 (D DC 2019) (dismissing negligence claim against insurer because parties had no special relationship). *Dolmage*, 2015 WL 292947, at *5 and *6 (dismissing with prejudice plaintiff 's negligence claim because Illinois law imposed no duty to safeguard PII in the absence of legislation imposing such a duty); *McConnell*, 828 S.E.2d at 358; *Jimmy John's*, 175 F. Supp. 3d 1064, 1071. Compare *Schnuck Markets*, 887 F.3d at 816 (breached supermarket owed no duty to banks under Illinois or Missouri law); *Citizens Bank of Pennsylvania v. Reimbursement Technologies, Inc.*, 609 F. App'x 88, 93 (3d Cir 2015).

11 See, e.g., *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 400 (ED Va 2020) (finding that bank had assumed a duty of care based on its actions); *Hapka*, 2016 WL 7336407, at *5 (finding duty under state law to exercise reasonable care to protect employee personal information where harm is foreseeable); *Dittman v. UPMC*, 196 A.3d 1036, 1047 and 1048 (Pa 2018) (finding employer had duty to use reasonable care to safeguard 'sensitive' employee information against potential breach where collected as a condition of employment).

12 See, e.g., *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.,* No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 and *4 (ND Ga 18 May 2016) (finding that defendants had a duty to safeguard PII but not expanding on the standard to meet that duty other than to note defendant's knowledge of a substantial security risk and failure to implement reasonable security measures constitutes a breach); compare *In re: Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *9 and *10 (ND Ga 5 Mar 2018) (finding that plaintiffs had sufficiently pleaded a beach of common law duty, in part, by alleging defendant failed to comply with standard industry security practices). Defining the contours of a 'reasonable' duty to safeguard PII may prove difficult, at least prospectively. See *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221, 1230,

a comparison of the conduct in question with 'industry practice' or 'industry standards', whereas defendants may note that 'reasonableness' at the time of the conduct in question must include an evaluation of whether the expected cost of safeguarding the information was outweighed by the benefit of doing so as perceived at the time relevant decisions were made. Outcomes (if fully litigated) will in any event be heavily dependent on the facts of each case.

Note that, in some states, the negligence line of attack can fall flat even if there is a clear duty of care. The economic loss doctrine generally provides that a contracting party alleging purely economic consequences (e.g., possible loss of future business) must seek a remedy in contract, not tort. Arguments for dismissal based on this doctrine are dependent on the doctrine's strength and contours in each state.[13]

Other common law theories

There are a number of other common law theories of liability usually found in class action complaints following a data security incident. However, the success rate for plaintiffs in bringing such claims is mixed at best.

For example, invasion of privacy claims are often dismissed because courts find there is no 'publication' of private information by the defendant.[14] Bailment claims are typically dismissed because plaintiffs cannot allege that they transferred their property to defendants, that defendants promised to return 'property' or that defendants wrongfully retained the information.[15] Misrepresentation claims often fail because plaintiffs rarely can allege that they justifiably relied on a false statement.[16] Finally, unjust enrichment claims usually, though not

---

1235 and 1236 (11th Cir 2018) (finding that the Federal Trade Commission's cease and desist order based on LabMD's failure to implement 'reasonable security measures to protect sensitive consumer information' to be unenforceable owing to vagueness).

13 Compare *Aguilar v. Hartford Accident & Indem. Co.*, No. CV 18-8123-R, 2019 WL 2912861, at *2 (CD Cal 13 Mar 2019) (dismissing negligence claim based on economic loss doctrine); *In re: Lenovo Adware Litig.*, No. 15-md-02624, 2016 WL 6277245, at *9 (ND Cal 27 Oct 2016) (dismissing negligence claims under New York and California law as barred by the economic loss doctrine), *Schnuck Markets*, 887 F.3d at 816 (dismissing negligence claim under Illinois law as barred by the economic loss doctrine), with *In re: The Home Depot, Inc.*, 2016 WL 2897520, at *3 (declining to dismiss negligence claim under Georgia law).

14 See, e.g., *Galaria v. Nationwide Ins. Co.*, 998 F. Supp. 2d 646, 661 and 662 (SD Oh 2014), rev'd on other grounds, No. 15-3386/3387 (6th Cir 12 Sep 2016) (dismissing claim when defendant did not publish plaintiffs' PII); *Smith v. Triad of Alabama, LLC*, No. 14-cv-324, 2015 WL 5793318, at *13 (MD Ala 29 Sep 2015) (same); but see *In re: Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 33 (DDC 2014) (finding plaintiff sufficiently pleaded invasion of privacy by alleging that her unlisted phone number and medical records were exposed by a data breach and that she had subsequently received unsolicited phone calls regarding her specific medical condition).

15 See, e.g., *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-cv-118; 2:13-cv-257, 2017 WL 6375803, at *3 and *4 (SD Oh 13 Dec 2017); *In re: Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D Minn 2014).

16 See, e.g., *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL, 2015 WL 4940371, at *5 and *6 (WD Wash 27 Mar 2015) (dismissing omissions-based misrepresentation claim); but see *In re: Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *38 (ND Cal 27 May 2016) (giving plaintiffs leave to amend fraudulent misrepresentation claim noting that allegations that plaintiffs 'viewed, heard, or read [d]efendants' privacy policies, and thus relied on the[ ] policies' would suffice to plead the claim).

always, fail because plaintiffs cannot allege they paid for cybersecurity protection[17] or because the existence of a contract (express or implied) prevents a parallel unjust enrichment claim.[18]

Consumer protection statute theories

State consumer protection statutes provide another source of claims that plaintiffs frequently use in bringing cases against breached companies. These statutes, while varying from state to state, commonly allow for claims based on any of three grounds: unlawfulness, unfairness or deception.

Unlawfulness claims, when available under state consumer protection statutes, typically require a showing that the conduct in question violates an established legal prohibition. No 'deception' or 'unfairness' is required; only that, for example, the conduct contravenes a particular statute.[19]

By contrast, unfairness claims under state consumer protection statutes require no showing of any specific statutory violation, but rather that the conduct in question is 'unfair'. Critically, most of these statutes provide little guidance as to what conduct qualifies. Some courts have looked to the factors that define 'unfairness' under Section 5 of the Federal Trade Commission (FTC) Act.[20] Other courts require that plaintiffs allege that a defendant's acts were (1) 'systematically reckless', (2) 'aggravated by [a] failure to give prompt notice', and (3) 'cause[d] widespread and serious consumer harm'.[21] Yet other courts, more troubling to

17 Compare *Community Bank of Trenton v. Schnuck Markets*, 887 F.3d 803, 820 (7th Cir 2018) (dismissing unjust enrichment claim), *Irwin v. Jimmy John's Franchise, LLC,* 175 F. Supp. 3d 1064, 1072 (CD Ill 2016) (same), with *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 411-12 (ED Va 2020) (denying motion to dismiss unjust enrichment claim), *Flynn v. FCA US LLC*, No. 15-CV-0855, 2017 WL 3592040, at *3 and *4 (SD Ill 21 Aug 2017) (same), *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1368 and 1369 (SD Fl. 2015) (same); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir 2012) (same). See also *In re: Target,* 66 F. Supp. 3d at 1177 and 1178 (rejecting overpayment theory but finding plaintiffs' unjust enrichment claim had merit on grounds that it was plausible plaintiffs 'would not have shopped' at Target had they known of the then-current breach).

18 Compare *Schnuck Markets,* 887 F.3d at 820 (dismissing unjust enrichment claim), *In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 984 (SD Cal 2014) [*Sony II*] (same), with *Fero v. Excellus Health Plan*, 236 F. Supp. 3d 735, 769 and 770 (WDNY 2017) (declining to dismiss unjust enrichment claim); *In re: Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *17 (ND Ga 5 Mar 2018) (same).

19 See, e.g., *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 989 (ND Cal 2016) ('Generally, violation of almost any law may serve as a basis for a [California unfair competition law] claim.') (quoting *Antman v. Uber Tech., Inc.*, 2015 WL 6123054, at *6 (ND Cal 19 Oct 2015) (citation omitted)).

20 See *Camacho v. Automobile Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006) (applying the FTC Act factors: '(1) the consumer injury must be substantial; (2) the injury must not be outweighed by any countervailing benefits to consumers or competition; and (3) it must be an injury that consumers themselves could not reasonably have avoided'); see also *In re: Anthem*, 162 F. Supp. 3d at 989 and 991.

21 *In re: Michaels Pin Pad Litig.*, 830 F. Supp. 2d 518, 526 (ND Ill 2011) (quoting *In re: TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 496 (1st Cir 2009)).

defendants, have declined to dismiss claims alleging merely 'unreasonable' or 'inadequate' cybersecurity,[22] or violations of 'established' public policy.[23]

Consumer protection statute claims based on 'deception' are similar to common law misrepresentation claims in that they often are premised on alleged materially misleading statements in user agreements[24] or alleged omissions about cybersecurity defects at the time of sale.[25] Contrary to their common-law counterparts, however, not all state consumer protection statutes require the plaintiff to allege or show reliance, and not all state consumer protection statutes require a resulting injury.[26]

Note also that state consumer protection statutes often impose other requirements or restrictions. For example, it is common for the statutes to require that the action arise from a sale of goods or services or a consumer-oriented practice.[27] It is also common that statutes limit relief to transactions that have a significant connection to the state.[28] Certain state statutes prohibit or restrict class relief (at least for actions brought and pending in the courts of that state).[29]

Other statute-based theories

Finally, class action complaints following a data breach can also include an array of allegations attempting to support causes of action asserted under other state or federal statutes. A main impetus for class action plaintiffs to assert such other statutorily based claims is that they

22 *In re: Home Depot, Inc. Cust. Data Sec. Breach Litig.*, No. 1:14-md-2583-TWT, 2016 WL 2897520, at *5 (ND Ga 18 May 2016); *In re: Target*, 66 F. Supp. 3d at 1162 (refusing to dismiss claim for failure to maintain 'adequate' data security practices).

23 See *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d. 953, 990 (ND Cal 2016).

24 *Grigsby v. Valve Corp.*, No. C12-0553JLR, 2013 WL 12310666, at *2 (WD Wash 18 Mar 2013); *Sony II*, 996 F. Supp. 2d at 985; *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 19 N.Y.S. 3d 850, 854 (NY Sup Ct 2015).

25 *Edenborough v. ADT, LLC*, No. 16-CV-02233-JST, 2016 WL 6160174, at *2 (ND Cal 24 Oct 2016); In re: Target, 64 F. Supp. 3d 1304, 1162 and 1163 (D Minn 2014); *In re: Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1229 (ND Cal 2014).

26 See, generally, *Sony II*, 996 F. Supp. 2d 942 (dismissing negligent misrepresentation claims and Michigan and Texas consumer protection claims for failure to plead reliance or causation, but allowing certain other claims under California, Missouri, Florida and New Hampshire statutes with lesser or no causation requirements); see also generally *In re: Experian Data Breach Litig.*, No. SACV 15-1592 AG, 2016 WL 7973595 (CD Cal 29 Dec 2016) (dismissing California statutory claims for failure to allege reliance and an Illinois fraud-based statutory claim for failure to allege causation, while allowing New York statutory claim based on mere showing of materiality); *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 996 and 997 (ND Cal 2016) (citing New York case in which a plaintiff's allegations supported the causation element of a deceptive-practices claim but did not support the reliance element needed for a common law claim).

27 *In re: Experian Data Breach Litig.*, 2016 WL 7973595, at *4 and *7; *In re: The Home Depot,* 2016 WL 2897520, at *5.

28 *Irwin v. Jimmy John's Franchise*, LLC, 175 F. Supp. 3d 1064, 1069 and 1070 (CD Ill 2016) ('A nonresident plaintiff may sue under the [Illinois Consumer Fraud and Deceptive Business Practices Act] only if the circumstances giving rise to the cause of action occurred "primarily and substantially in Illinois".'); *In re: Sony Gaming Networks and Cust. Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 964 and 965 (SD Cal 2012) [*Sony I*] (dismissing non-resident plaintiffs' claims brought under California statutes).

29 See *In re: Anthem*, 162 F. Supp. 3d 953, 999 and 1000; *In re: Target*, 64 F. Supp. 3d at 1163; *Sony II*, 996 F. Supp. 2d 942, 1003.

often provide for statutory damages, which if applied per class member on a class-wide basis, raise the prospect of huge damage awards.

For example, the Fair Credit Reporting Act (FCRA) requires 'reasonable procedures' as to the handling of consumer reports in certain respects[30] and includes a private right of action permitting recovery of between US$100 and US$1,000 in statutory damages per violation of the statute generally.[31] Plaintiffs in a variety of breach cases have thus invoked the FCRA to seek class-wide relief in an effort to obtain statutory damages.[32] The Stored Communications Act (SCA) also provides for statutory damages, at a minimum of US$1,000 per violation, although some courts have recognised that plaintiffs may claim the statutory amount only upon a showing of having incurred at least some actual damage as well.[33] To date, however, courts in data breach cases have usually found that those statutes target specified harms other than those underlying the claims in question. Claims under the FCRA, thus, have been rejected in the data breach context because the statute applies only to 'consumer reporting agencies' and addresses only 'furnishing' of data.[34] Similarly, alleged violations of the SCA have been rejected because the statute applies only to covered providers of covered communications who 'knowingly divulge'[35] the data in question.[36] Claims based on the violation of other federal statutes imposing data security requirements or restricting disclosure of personal information also fail if the relevant statute does not provide a private right of action.[37]

---

30 15 USCA Section 1681e(a).

31 Note that if a person knowingly violates the statute, liability increases to the greater of actual damages sustained by the consumer or US$1,000. 15 USCA Section 1681n(a)(1)(A) and (B).

32 See, e.g., *Tierney v. Advocate Health & Hosps. Corp.*, 797 F.3d 449, 450 (7th Cir 2015); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1313 (ND Ga 2019); *Sony II*, 996 F. Supp. 2d at 959.

33 18 USCA Sections 2702 and 2707(c); *Vista Marketing, LLC v. Burkett*, 812 F.3d 954, 965 and 967 (11th Cir 2016) (interpreting the language of the statute to provide damages only to plaintiffs who experienced actual damages); but see *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1045 (ND Cal 2018) (noting that district courts in the Ninth Circuit have held that plaintiffs can obtain damages under the SCA without a showing of actual damages).

34 See, e.g., *Tierney*, 797 F.3d at 451 and 452; *Sony II*, 996 F. Supp. 2d at 1011; *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1312 (ND Ga 2019).

35 18 USCA Section 2702(a)(1) to (3).

36 *In re: Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752, 2017 WL 3727318, at *41 and *42 (ND Cal 30 Aug 2017) (plaintiffs failed to allege that defendants knowingly divulged any information); *Burrows v. Purchasing Power*, LLC, No. 12-CV-22800, 2012 WL 9391827, at *4 and *5 (SD Fla 18 Oct 2012) (plaintiff failed to plead facts showing that defendant was a covered entity under the SCA or that defendant knowingly divulged plaintiff's PII).

37 See, e.g., *In re: Anthem, Inc. Data Breach Litig,* 162 F. Supp. 3d, , 897 and 898, 980 and 981 (ND Cal 2016) (claim failed because the Health Insurance Portability and Accountability Act of 1996 [HIPAA] has no private right of action); *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1368 and 1369 (SD Fla 2015) (same); *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 19 N.Y.S. 3d 850, 859 (NY Sup Ct 2015) (same under the Health Information Technology for Economic and Clinical Health Act). But see *In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1202 and 1203 (D Or 2016) (lack of a private right of action under HIPAA did not preclude causes of action under state law even if an element of the state claim required showing a HIPAA violation). Well-pleaded violations of these statutes have in some instances survived motions to dismiss if styled as causes of action for negligence *per se*. Compare *First Choice Fed. Credit Union v. Wendy's Co.*, No. CV 16-506, 2017 WL 9487086, at *3 and *4 (WD Pa 13 Feb 2017), report and recommendation adopted, No. CV 16-506, 2017 WL 1190500 (WD Pa 31 Mar 2017) (declining to dismiss negligence *per se* claim premised on alleged violation of the FTC Act), with *Community Bank of Trenton v.*

In addition to federal statutes, plaintiffs may attempt to assert claims under various state laws. As of 2018, all 50 states and the District of Columbia have data breach notification statutes of varying scope.[38] Yet even when those statutes provide a private right of action,[39] claims for insufficient or untimely notice often fail for lack of claimed injury stemming from the insufficiency or untimeliness itself.[40] Similarly, a number of state statutes also include provisions imposing security standards with respect to protecting personal information[41] and some permit private rights of actions to be asserted – either directly or indirectly – for non-compliance.[42]

The landscape of state statutes changed dramatically in January 2020 when the California Consumer Privacy Act (CCPA) became operational. The CCPA provides a private right of action to California consumers[43] for certain failures to maintain 'reasonable security' resulting in a data breach and, significantly, provides for statutory damages of between US$100 and US$750 'per consumer per incident'.[44] The statute provides defendants an opportunity to cure any breach within 30 days, but it is unclear in practice how defendants would do so. Private litigation invoking the CCPA has begun, though as of yet decisions interpreting the CCPA are sparse. Defendants have raised questions concerning the scope and application of the private right of action, such as whether it applies retroactively to incidents before 1 January 2020[45] and whether defendants were provided adequate notice and opportunity to cure.[46] Defendants have also raised arguments regarding whether the data at issue is 'personal

Schnuck Markets, 887 F.3d 803, 819 n.7 (7th Cir 2018) (dismissing negligence *per se* claim based on alleged violation of the FTC Act).

38 See Security Breach Notification Laws, Nat'l Conf. of State Legs. (19 Sep 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

39 The Alabama statute, for example, expressly states that it does not provide for a private right of action. 2018 Ala. Laws Act 2019-396 Section 9(a)(1) (SB 318) (setting forth notification requirements in the event of a data breach but expressly noting that '[a] violation of this act does not establish a private cause of action').

40 See, e.g., *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1253 to 1255 (D Colo 2018) (claim under state breach notification statute for failing to promptly notify customers dismissed as to plaintiffs who had learned of and taken action regarding fraudulent transactions before defendant learned of breach, and who thus could not allege harm due to delay in notice); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 16-MD-02752, 2017 WL 3727318, at *37 and *38 (ND Cal 30 Aug 2017) (dismissing delay claim by Yahoo! plaintiffs for 2013 breach because liability arises only from delay and not from breach itself, and plaintiff failed to allege when 2013 breach was discovered); ibid., at *40 and *41 (discussing other cases in which delay claims failed for lack of direct injury, but holding that delay claims by Yahoo! plaintiffs as to 2014–2016 breaches adequately alleged a direct connection between alleged incremental damages and the claimed delay).

41 See Data Security Laws – Private Sector, Nat'l Conf. of State Legs. (4 Jan 2019), www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

42 Ca. Civil Code, Section 1798.81.5(b); Ill. Comp. Stat. 815 ILCS 530/45(a); Md. Code. Ann. Com. Law 14-3503(a).

43 Ca. Civil Code, Section 1798.140(g) (defining 'consumer' as 'a natural person who is a California resident').

44 Ca. Civil Code, Section 1798.155(b).

45 See, e.g., *Gardiner v. Walmart, Inc.*, No. 4:20-cv-04618-JSW (ND Cal 5 Mar 2021) (dismissing claim because breach may have occurred before 1 January 2020).

46 See, e.g., *Guzman v. RLI Corp. et al.,* No. 2:20-cv-08318 (CD Cal 22 Oct 2020) (Doc. 26-1) (arguing plaintiff did not comply with notice and cure provision).

information', which is defined more narrowly with respect to the private right of action than under the statute as a whole.[47]

At the close of 2020, California voters passed a ballot initiative, Proposition 24, known as the California Privacy Rights Act (CPRA) that will go into operation in 2023. Of relevance to the data-breach cause of action, it will eliminate the right to cure. Legislative proposals are also pending in other states that may include new rights of action.[48]

Emerging trends in litigation: securities litigation

While the most common cybersecurity actions continue to be class actions brought by individuals whose information was allegedly compromised under the foregoing theories, recent years have seen an increase in shareholder derivative and securities fraud actions as well.

Shareholder derivative actions

Shareholder derivative actions have followed most prominent data breaches since at least the Target breach in 2013. In these actions, plaintiffs allege that directors and officers breached their fiduciary duties, committed gross mismanagement, wasted corporate assets or abused their control in failing to oversee the company's cybersecurity posture.[49] Thus far, plaintiffs have had limited success with these allegations,[50] with one some exceptions.[51]

Defendants often succeed in dismissing shareholder derivative actions because plaintiffs must plead with particularity that either (1) the board of directors wrongfully refused to bring the suit, or (2) it would have been futile to request that the board bring such an action.[52] This leaves plaintiffs in a challenging position. Under Delaware law, if plaintiffs ask the board to bring the action, when the board says no (which is likely to be the case), the plaintiff must prove the board's decision was outside the bounds of the business judgement

47 See, e.g., *Walmart, Inc.*, No. 4:20-cv-04618-JSW (ND Cal 5 Mar 2021) (finding failure to allege disclosure of personal information meeting definition under privacy right of action).

48 See, e.g., SD 341, 2019 Sen., 191st Sess. (Mass 2019); SB 179, 54th Leg., Reg. Sess. (NM 2019); S. 0234, 2019 Gen Assembly (RI 2019).

49 See, e.g., Complaint at paras. 3 to 7, *Davis v. Steinhafel*, No. 14-cv-00203 (D Minn 21 Jan 2014); *In re: The Home Depot Inc. S'holder Derivative Litig.*, 223 F. Supp. 3d 1317 (ND Ga 2016).

50 See, e.g., *Corp. Risk Holdings LLC v. Rowlands*, No. 17-cv-5225(RJS), 2018 WL 9517195, at *6 (SDNY 28 Sept 2018) (dismissing claims of breach of fiduciary duty where plaintiffs plead 'nothing more than industry-wide generalisations about cybersecurity risks, not company-specific evidence of misconduct or compliance failure necessary to sustain a claim for director liability'.).

51 *In re Equifax Inc. Securities Litigation*, 357 F.Supp.3d 1189 (ND Ga 2019) (denying motion to dismiss claims against Equifax's former CEO and chairman of the board based on allegations of personal knowledge of inadequate cybersecurity practices, and knowingly and recklessly making false and misleading about Equifax's data security). Similarly, in the matter *In re: Yahoo! Inc. Shareholder Litigation*, No. 17-cv-307054 (ND Cal 9 Jan 2019), the court approved an US$29,000,000 shareholder settlement on 9 Jan 2019. The settlement marked the first time that shareholders were awarded monetary damages in a derivative lawsuit relating to a data breach.

52 See Fed. R. Civ. P. 23.1(b)(3); *Palkon v. Holmes*, No. 2:14-CV-01234 SRC, 2014 WL 5341880, at *2 (DNJ 20 Oct 2014) (plaintiff brought suit alleging board wrongfully refused to bring action); Complaint at para. 7, *Graham v. Peltz*, No. 1:16-cv-1153 (SD Oh 16 Dec 2016) (plaintiff alleged that it would have been futile to request the board bring the action); *In re: the Home Depot*, 223 F. Supp. 3d at 1324 (same).

rule – an exceedingly difficult task.[53] However, if the plaintiffs argue that demand would be futile, they have to show that the majority of directors were conflicted owing to a significant likelihood that the directors faced individual liability or that the board failed to inform themselves to the extent appropriate under the circumstances.[54]

Stock purchase class action complaints

Securities fraud litigation following a data security incident is also on the rise. In fact, in 2017 and 2018, plaintiffs filed 23 federal securities class actions based on a data security incident, compared to zero in 2016.[55] The widely publicised data breach at Marriott International (Marriott) demonstrates how popular these types of actions had become by the end of 2018. Marriott publicly announced that it had suffered a data security incident on Friday, 30 November 2018, and the first securities class action lawsuit was filed the next day.[56] Similarly, in 2019 and 2020, plaintiffs continued to file such class actions with respect to notable data security incidents including the Capital One breach.[57]

While complaints like the one filed in Marriott frequently lack extensive *scienter* allegations, and sometimes even lack evidence of a significant drop in stock price, plaintiffs' lawyers hope to defeat a motion to dismiss by alleging two (non-exclusive) theories. First, plaintiffs, like those in *Marriott*,[58] will allege that public statements were materially false or misleading because the company overstated its cybersecurity abilities, or otherwise failed to inform investors that the company was susceptible to a cyberattack.[59] Second, similar to a traditional

53 See, e.g., *Palkon*, 2014 WL 5341880, at *3 (dismissing claims under Delaware law because plaintiffs failed to plead reasonable doubt regarding business judgement rule); *Zapata Corp. v. Maldonado*, 430 A.2d 779, 785 (Del 1981) ('To allow one shareholder to incapacitate an entire board of directors merely by leveling charges against them gives too much leverage to dissident shareholders.') (citation omitted).

54 See, e.g., *In re: The Home Depot*, 223 F. Supp. 3d at 1325 (stating the Delaware law requirement for testing board's independence as a showing that board engaged in conduct 'so egregious on its face that board approval cannot meet the test of business judgment, and a substantial likelihood of director liability therefore exists'). See also *Marx v. Akers*, 666 N.E. 2d 1034, 1040 (NY Ct App 1996) (stating demand excuse requirements under New York law).

55 'Securities Fraud Claims Get Boost from EU Data Privacy Rules', Bloomberg Privacy & Security Law Report (BNA) (1 Feb 2019).

56 Complaint, *McGrath v. Marriott International, Inc.*, No. 18-cv-06845 (EDNY 1 Dec 2018) [*Marriott* Complaint]. Notably, the first consumer class action was filed even more quickly – on 30 November 2018, the same day the breach was announced.

57 *Minsky v. Capital One*, No. 1:19-cv-05594 (EDNY 2 Oct 2019); for a broader list, see *The Stanford Law School Securities Class Action Clearinghouse*. Stanford Law School, https://securities.stanford.edu/current-topics.html#collapse1 (last visited 10 March 2021).

58 The *Marriott* plaintiffs alleged that Marriott's Form 10-Q filed with the Securities and Exchange Commission gave the 'misleading impression' that systems storing customer data were secure. *Marriott* Complaint, at paras. 17 to 22. News of the breach broke before trading opened on 30 November 2018; by the end of the trading day, Marriott's stock fell more than 5.5 per cent; ibid., at paras. 24 and 25.

59 See *Kim v. Advanced Micro Devices, Inc.*, No. 18-cv-00321, 2018 WL 2866666, at *1 (ND Cal 11 Jun 2018); *In re: Equifax Inc. Sec. Litig.*, No. 17-cv-3463, 2019 WL 337807, at *9 (ND Ga 28 Jan 2019); Complaint at para. 4, *In re: Intel Corp. Sec. Litig.*, No. 18-cv-00507 (ND Cal 23 Jan 2018) [*In re: Intel Corp*. Complaint]; *Marriott* Complaint, at para. 23.

consumer class action, plaintiffs will allege that the company knew about a cyberattack, but did not disclose it to the market in a timely manner.[60]

While not necessary to bring a securities fraud action, allegations of insider stock sale prior to the public disclosure of the breach can accompany Section 10b-5 claims.[61]

Key strategic considerations in litigation

Non-litigation focused decisions made after a cyberattack may be critical

After a cyberattack, an affected party may want to reassure partners, customers and the general public that any damage was minimal, that it has strong cybersecurity to prevent further attacks, and that it will mitigate the harm caused. However, such actions taken in the first few days (or even hours) of learning of a breach can have a profound effect on litigation that will inevitably follow, and thus those actions must be considered carefully.

A company that is aware of a data security incident should pay special attention to any public statements about the company's data security. This includes statements in routine public filings. As noted above, deception and implied contract-based claims turn, in part, on the company's statements relating to its data security. As a result, when considering whether and how much to disclose, companies should be mindful that the disclosures may eventually be cited in support of an allegation that the company overstated or misled consumers as to its practices.

When a company has disclosed a data security incident, it should be equally cautious about how it describes the extent of a breach. While defendants have had success in challenging plaintiffs' standing to bring suit, recent court decisions demonstrate that a company's public comments can undercut arguments regarding a lack of standing as a ground for dismissal. For example, in the aftermath of a breach, Zappos urged 'affected customers to change their passwords on any other account where they may have used the same or similar password' as for their Zappos account.[62] The Ninth Circuit pointed to that statement to establish that the plaintiffs sufficiently alleged an injury based on a substantial risk that the hackers would commit identity fraud or theft.[63]

Another hard question a company may face after a breach is deciding whether to offer affected customers free credit monitoring.[64] This is often seen as good customer service (and, depending on the circumstances and the information affected, may be required by a number of state data breach notification laws). From a litigation perspective, if there is harm, credit monitoring could mitigate it, and some courts have found that free credit monitoring elimi-

60 *In re: Equifax*, 2019 WL 337807, at *14 and *15.

61 See, e.g., Amended Consolidated Complaint at para. 199, *In re: Equifax Inc. Sec. Litig.*, No. 17-cv-3463 (ND Ga 14 May 2018) (alleging that three high-level executives sold millions of dollars of Equifax stock before publicly disclosing the incident); *In re: Intel Corp*. Complaint at para. 9 (alleging that Intel's Chief Executive Officer sold US$24 million worth of the company's stock and options after Intel was informed of data security vulnerabilities but before that information was disclosed publicly).

62 *In re: Zappos.com, Inc.*, 888 F.3d 1020, 1027 and 1028 (9th Cir 2018) (quotation marks and footnote omitted).

63 ibid., at 1029.

64 Note that, in a few states, an offer of some period of identity protection or remediation services to residents of those states is in any event now required by statute for a set period of years. Conn. Gen. Stat. Ann. Section 36a-701b(b)(2)(B) (two years); Del. Code Ann. tit. 6, Section 12B-102(e) (one year); Mass. H. 4806 (2018) (18 months).

nates the need for plaintiffs to purchase their own and thus removes one means by which a plaintiff can demonstrate injury-in-fact.[65] However, some courts have treated an offer for free credit monitoring as an admission that consumers face a substantial risk of harm.[66] Notably, some courts that take the former view observe that to use an offer of credit monitoring to establish standing would discourage organisations from offering these services.[67]

Finally, in the aftermath of a cyberattack, and as discussed further in Chapter 3 on The 'Art' of Investigating, a company is likely to want to (and should) act quickly to investigate the cause of the attack and its potential ramifications. However, the structure of any internal investigation – whether it is intended to inform counsel in providing legal advice or for a different purpose – may affect whether related documents and communications are protected by the attorney–client privilege or work-product doctrine. A company responding to a breach should therefore consider designing and executing an internal investigation to protect the company's claim to privilege to the fullest extent.[68] In particular, a company should consider recent decisions regarding the application of the work-product doctrine and attorney–client privilege to forensic reports generated by third parties when determining how to structure an investigation and engage a third party.[69]

Judicial Panel on Multidistrict Litigation

In the wake of a large data breach in particular, corporations should anticipate that actions will be filed in multiple jurisdictions and should devise strategies to consolidate those actions in a jurisdiction with laws that are the most appropriate for the case.

When cases are filed in a single judicial district, judges frequently entertain motions to consolidate. When cases are filed in multiple jurisdictions – a common occurrence when the pool of potential plaintiffs is geographically diverse – a defendant or plaintiff can seek to transfer and consolidate the federal cases before one district court for pretrial purposes via a centralisation motion filed with the Judicial Panel on Multidistrict Litigation (JPML). The seven circuit and district judges on the JPML, appointed by the Chief Justice of the United States, have the authority to transfer federally pending cases involving 'common questions

65 *Falkenberg v. Alere Home Monitoring, Inc*., No. 13-341, 2014 WL 5020431, at *4 (ND Cal 7 Oct 2014) (dismissing claims under California law).

66 *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir 2016) ('Nationwide seems to recognize the severity of the risk [of fraud and identity theft], given its offer to provide credit-monitoring and identity-theft protection for a full year.'). Query if that rationale holds where the offer is required by statute. See footnote 58 and accompanying text.

67 *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir 2017).

68 Compare *In re: Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522, 2015 WL 6777384, at *2 and *3 (D Minn 23 Oct 2015).

69 See, e.g., *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2015 WL 6777384, at *1-2 (D Minn 23 Oct 2015 (holding the attorney client privilege and work product document applied to communications from third-party forensic consultant retained to assist counsel in conducting investigation); *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190–93 (MD Tenn 2014) (same). But see *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 3470261 (ED Va 25 June 2020) (holding work product doctrine did not protect forensic report Capital One argued was prepared for counsel); *Guo Wengui v. Clark Hill*, PLC, et al., 2021 WL 106417 (DDC 2021) (finding the same with respect to the work product doctrine and attorney–client privilege).

of fact' for consolidated or coordinated pretrial proceedings.[70] The jurisdiction of the JPML, however, does not extend to cases pending in state court. Therefore, unless the state cases are removable to federal court, defendants may be forced to litigate the same claims on two fronts, or at least incur additional expenses seeking to coordinate proceedings across the federal and state systems.[71]

Choice of law variances

The importance of the state law applied to a data breach litigation cannot be overstated. For example, in November 2018, the Supreme Court of Pennsylvania held in *Dittman v. UPMC* that an employer has a legal duty to exercise reasonable care to safeguard the sensitive personal information about employees that is stored on any internet-accessible computer system.[72] In contrast, Illinois cases have declined to impose any duty to safeguard PII from disclosure[73] and the Georgia Court of Appeals has similarly found no duty under Georgia law to safeguard personal information.[74] The *Dittman* court further held that Pennsylvania's economic loss doctrine provides recovery for purely pecuniary damages under a negligence theory, provided that the plaintiff can establish the defendant's breach under common law is independent of any duty assumed pursuant to contract.[75] Unlike Pennsylvania, courts applying New York and California law find that the economic loss doctrine bars negligence claims for purely pecuniary damages.[76]

Interestingly, choice of law provisions sometimes require one court to apply the law of multiple states in the same action. This can happen, for example, when geographically diverse plaintiffs were all injured in their home states. Defendants in class actions generally are starting to point to these plaintiff-specific variances to defeat class certification under Federal Rule of Civil Procedure 23(b)(3), which permits class actions only if 'the court finds that the questions of law or fact common to class members predominate' over those affecting only

70 28 USC Section 1407(a). See, e.g., *In re: Marriott International, Inc., Customer Data Sec. Breach Litig.*, No. MDL 2879, 2019 WL 623593 (JPML 6 Feb 2019) (centralising both consumer class actions and stockholder securities actions stemming from Marriott's data security incident).

71 See, e.g., *In re: Uber Techs., Inc., Data Sec. Breach Litig.*, 304 F. Supp. 3d 1351, 1354 (JPML 2018) (granting centralisation of pending federal data breach class actions in single federal district, while noting the continuing pendency of parallel state court actions).

72 *Dittman v. UPMC*, 196 A.3d 1036, 1047 (Pa 2018).

73 *Cooney v. Chicago Pub. Sch.*, 943 NE 2d 23, 28 and 29 (Ill App Ct 2010); see also *In re: SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *14 (D Minn 7 Mar 2018) ('Federal courts interpreting Illinois law have consistently declined to impose a common law duty to safeguard personal information in data security cases.' (citation omitted)).

74 *McConnell v. Dep't of Labor*, 828 S.E.2d at 358 (Ga 2019); but see *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (ND Ga 18 May 2016) (footnotes omitted).

75 *Dittman*, 196 A.3d at 1056.

76 See footnote 13 and accompanying text.

individual members.[77] Given the range of differences between the common law and statutory causes of action asserted by plaintiffs, the same rationale would apply in data breach cases.[78]

Class certification timing

Class certification, and the timing of it, can also have a significant effect on a case. Some courts are willing to bifurcate class certification discovery and merits discovery. If a defendant believes that it can successfully defeat class certification,[79] it can save significant time and money by using bifurcated discovery and having class certification addressed early. If the defendant wins on its opposition to class certification, it may be able to settle the action with the named plaintiffs for a minimal amount, avoiding expensive discovery on merits issues collateral to the class certification issue itself.[80]

However, plaintiffs' lawyers are often reluctant to agree to an early ruling on class certification, lest they cede the settlement leverage that the cost and burdens of discovery may afford them in the interim. Accordingly, they will frequently oppose bifurcating discovery and argue that class certification is so intermingled with the merits of the case that full discovery is required before any motions are filed.[81]

77 See *In re: Hyundai & Kia Fuel Econ. Litig.*, 881 F.3d 679, 691 to 693, 703 (9th Cir 2018), rehearing *en banc* granted *sub nom. In re: Hyundai And Kia Fuel Econ. Litig.*, 897 F.3d 1003 (9th Cir 2018) (in a putative class action regarding car manufacturers' alleged misstatements about fuel efficiency, the Ninth Circuit found that the district court abused its discretion by (1) failing to acknowledge that the laws in various states were materially different from those in California, and (2) not ruling on whether the variations would defeat predominance); *Langan v. Johnson & Johnson Consumer Cos., Inc.*, 897 F.3d 88, 98 (2d Cir 2018) (in a putative class action against the seller of baby bath products, the Second Circuit noted that the party seeking class certification has the ultimate burden of demonstrating that any variances in state laws do not predominate and that the district court must engage in a rigorous analysis of the similarities and differences in the relevant laws).

78 See, e.g., *In re: Conagra Peanut Butter Prod. Liab. Litig.*, 251 F.R.D. 689, 699 (ND Ga 2008) ('It goes without saying that class certification is impossible where the fifty states truly establish a large number of different legal standards governing a particular claim.') (quotations omitted); but see Memorandum and Order at 5 to 9, *In re: Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522 (D Minn 15 Sep 2015) (rejecting argument that because negligence claims are subject to laws of different states class treatment of those claims is inappropriate). For an example of when questions of fact did not predominate the class, see *In re: TJX Companies Retail Sec. Breach Litig.*, 246 F.R.D. 389, 395 and 396 (D Mass 2007).

79 See, e.g., *McGlenn v. Driveline Retail Merch., Inc.*, 2021 U.S. Dist. LEXIS 9532, 15 (CD Ill. Jan. 19, 2021) (denying data breach class certification, in part, because 'issues of causation and injury require individual inquiry').

80 See *Harris v. comScore, Inc.*, No. 11 CV 5807, 2012 WL 686709 (ND Ill 2 Mar 2012) (bifurcating class certification discovery from merits discovery in class action involving alleged collection and dissemination of personal information in violation of state and federal laws). See also Manual for Complex Litigation (Fourth) Section 21.14 (2018).

81 Compare *New England Carpenters Health & Welfare Fund v. Abbott Labs*, No. 12 C 1662, 2013 WL 690613, at *3 (ND Ill 20 Feb 2013) (denying bifurcation, accepting plaintiff's argument that 'merits and class certification issues inevitably overlap, bifurcation will serve only to needlessly protract this litigation') (internal quotations and citation omitted), with *comScore*, 2012 WL 686709 (granting bifurcation, rejecting plaintiffs' arguments regarding 'delay' and anticipated disagreements about the 'permissible scope of class certification discovery').

Current range of holdings on injury requirements

As with all plaintiffs seeking to bring litigation in a US federal court, data breach plaintiffs must allege an injury-in-fact sufficient to confer standing under Article III of the US Constitution.[82] Article III limits the jurisdiction of federal courts to cases or controversies in which the plaintiff demonstrates that he or she has suffered (1) an injury-in-fact (2) that is fairly traceable to the defendant's actions and (3) is likely to be redressed by the relief sought from the court.[83] In this section, we discuss two recent landmark Supreme Court decisions on Article III's injury-in-fact requirement and the resulting circuit splits regarding injury needed to sufficiently plead standing in data breach cases in federal court. This section also considers how – even when standing is satisfied – different claims of injury fare in alleging the requisite elements of the cause of action itself.

Standing: current versus future injury

Under the Supreme Court's 2013 ruling in *Clapper v. Amnesty International USA*, to establish injury-in-fact, plaintiffs must allege injury that has already accrued or threatened injury that is 'certainly impending'.[84] This decision notes that a plaintiff cannot manufacture current injury by spending money to avoid future harm, if that future harm itself is not certainly impending.[85] Circuits have subsequently split over the decision's application in litigation resulting from a data breach.

Four circuits – the D.C., Sixth, Seventh and Ninth – have held that individuals whose personal information is held in a database breached by hackers have Article III standing by virtue of substantial risk of future out-of-pocket injury.[86] As explained by the DC Circuit: 'simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken', plaintiffs have experienced a substantial risk of harm that is sufficient to establish injury.[87] In contrast, under a range of factual circumstances, the First, Second, Third, Fourth and Eighth Circuits have held that the mere risk of data misuse is too speculative to create standing

82 Note that constitutional standing concerns do not arise in shareholder derivative or stock purchase cases, since the ownership or purchase of the stock in and of itself suffices to provide standing to challenge the actions of the company or its officers and directors with respect to the breach in question. Fed. Rule Civ. Pro. 23(b)(1) (detailing standing requirements to bring a derivative action); *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, 753 and 754 (1975) (finding Congress intended to limit standing in cases brought under the Exchange Act to plaintiffs who had purchased stock).

83 *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

84 *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1143 (2013).

85 ibid., at 1151; see also *Stasi v. Inmediata Health Grp. Corp.*, No. 19cv2353 JM (LL), 2020 WL 2126317, at *9 (SD Cal 2020) ('Plaintiffs cite no case in which the expenditure of time or money to prevent future identity theft was sufficient in and of itself to support standing without a finding that the threat of identity theft was imminent.').

86 *Attias v. CareFirst*, 865 F.3d 620, 629 (DC Cir 2017); *In re Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 54-61 (DC Cir 2019); *Galaria v. Nationwide Mutual Ins. Co*., 663 F. App'x 384, 388 and 389 (6th Cir 2016); *Remijas v. Neiman Marcus Grp. LLC*, 794 F.3d 688, 693 (7th Cir 2015); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir 2016); *In re: Zappos.com*, 888 F.3d 1020, 1025 and 1026 (9th Cir 2018); see also *In re: Horizon HealthCare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 630, 638 and 639 (3d Cir 2017) (finding standing based on de facto injuries under a federal privacy law).

87 *Attias*, 865 F.3d at 629.

because no injury is 'certainly impending' nor is there a 'substantial risk' of injury.[88] The Eleventh Circuit has held similarly in an unpublished decision.[89]

Standing: tangible versus intangible injury

The Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins* addressed a slightly different question: what makes an injury sufficiently concrete to confer standing. The Court explained that, to be concrete, the injury must 'actually exist' and that 'risk of real harm' could satisfy the concreteness standard.[90]

While out-of-pocket loss that is actually and already incurred is considered sufficient tangible harm to establish injury-in-fact, other alleged injuries have been found intangible and insufficient to confer standing. For example, some courts find that alleged anxiety, inconvenience and lost time caused by a data breach are not particularised and are not sufficiently concrete to confer standing, though that finding is not universal.[91] Courts often reject standing based on a diminished value of PII; although, some recent decisions have accepted the theory.[92]

Increasingly, plaintiffs allege they have suffered a concrete harm because they 'overpaid' for a good or service. This theory is premised on the idea that because the purchase of goods or services created the circumstances in which the purchaser's personal data was potentially affected by a subsequent breach, the purchaser overpaid for the goods or services.[93] The overpayment theory is attractive to plaintiffs because, apart from standing, it may also provide a basis for establishing uniform damages across the class. Yet if the plaintiff fails to allege any defect in the product or service itself, or that security itself was identified as part of the

88 See *Katz v. Pershing*, LLC, 672 F.3d 64, 80 (1st Cir 2012); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir 2017); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42-43 (3d Cir 2011) (no standing under common law principles); *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir 2017); *In re: SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir 2017).

89 *Tsao v. Captiva MdVP Restaurant Partners*, 2021 U.S. App. LEXIS 3055 (11th Cir 4 Feb 2021).

90 *Spokeo*, 136 S.Ct. 1540, 1548 and 1549.

91 Compare, *Whalen*, 689 F. App'x at 90; *Fero v. Excellus Health Plain, Inc.*, 236 F. Supp. 3d 735, 754 (WDNY 2017), on reconsideration *sub nom. Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333 (WDNY 2018), with *Bass v. Facebook*, 393 F. Supp. 3d 1024, 1034 (ND Cal 2019 (loss of time in responding to breach sufficient for standing).

92 *In re Uber Techs., Inc., Data Sec. Breach Litig.*, No. CV182970PSGGJSX, 2019 WL 6522843, at *5 (CD Cal 19 Aug 2019) (rejecting diminution of value theory where plaintiff had not established an impairment of his ability to participate in that market for personal information); *Mount v. PulsePoint, Inc.*, No. 13 CIV. 6592, 2016 WL 5080131, at *6 (SDNY 17 Aug 2016), aff'd, 684 F. App'x 32 (2d Cir 2017), as amended (3 May 2017) (rejecting diminished value of PII theory on grounds that it was too conjectural); *Khan v. Children's Nat'l Health System*, 188 F. Supp. 3d 524, 533 (D Md 2016) (allegation that data breach diminished the value of PII rejected as a theory to support standing because the breach did not deprive plaintiff of her PII). But see *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG (DFMx), 2016 WL 7973593, at *5 (CD Cal 29 Dec 2016) ('A growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory.').

93 See *Lewert*, 819 F.3d at 968 (product itself must be defective and purchaser must claim they would not have bought it had they known of the defect); *Neiman Marcus,* 794 F.3d at 694 (noting in *dicta* that it is 'dubious' overpayment allegations alone suffice for standing).

product or service being purchased, efforts to use allegations of 'overpayment' alone to satisfy standing in data breach cases have so far not had great success.[94]

Alleging solely the violation of a statute to establish standing, moreover, could suffice under *Spokeo* if (1) there is a 'close relationship' between the harm alleged and 'a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts'; and (2) the statute being enforced reflects Congress' judgment that the alleged harm meets minimum Article III requirements.[95] Acknowledging that Congress can elevate an intangible harm to a concrete injury through legislation, the Third Circuit currently leaves open the possibility of rejecting 'mere technical violations' of a statutory procedural requirement in determining injury-in-fact.[96] In any event, standing after *Spokeo* continues to be a significant jurisdictional issue that federal courts must consider and address and that can be raised at any level of litigation.[97]

Actionable injury: sufficiency for the cause of action

The fact that a plaintiff's injury is sufficient to confer Article III standing does not mean it is sufficient to state a claim for damages under Rule 8(a)(2) of the Federal Rules of Civil Procedure. Indeed, separate and apart from standing issues, and even if the theories of liability as laid out in 'Typical causes of action in US litigation' (above) are otherwise sustained, a notable stumbling block for many cybersecurity plaintiffs has long been, and continues to be, the failure to allege injury sufficient to state a claim.[98] For example, costs incurred from actual misuse of stolen information have been held actionable only if there is an actual out-of-pocket loss.[99] A mere increased risk of future identity theft can be rejected as insufficient as actionable injury,[100] while credit monitoring costs, lost time and other mitigation measures

94 See, e.g., *Lewert*, 819 F.3d at 968 (failing to allege defect); *Neiman Marcus*, 794 F.3d at 694 (same); *Cox v. Valley Hope Ass'n*, No. 16-CV-04127-NKL, 2016 WL 4680165, at *3 and *4 (WD Mo 6 Sep 2016) (failing to allege that defendant represented cost of services as including data security measures).

95 *Spokeo*, 136 S.Ct. at 1549 (citations omitted).

96 *In re: Horizon HealthCare Servs. Inc. Data Breach Litig.*, 846 F.3d at 638 to 641 (court does not opine on the types of 'mere technical violations' that would be insufficient to confer standing).

97 After granting writ of *certiorari* and hearing oral arguments in *Frank v. Gaos*, the Supreme Court declined to reach the merits of the case, instead remanding it to the courts below to address plaintiffs' standing in light of *Spokeo. Frank v. Gaos*, 139 S.Ct. 1041, 1046 (2019) (*per curiam*).

98 See, e.g., *Kuhns v. Scottrade*, 868 F.3d 711, 716 and 717 (8th Cir 2017) (plaintiffs with Article III standing nevertheless failed to allege harm sufficient to state a breach of contract claim); *Krottner v. Starbucks Corp.*, 406 Fed. App'x 129, 131 (9th Cir 2010) (same for claim of negligence); *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500, at *6 and *7 (ND Ill 14 July 2014) (same for breach of contract and consumer fraud claims); but see *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir 2018) ('To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available.').

99 See, e.g., *Sony I*, at 942, 962 and 963 (plaintiffs' negligence claim failed due to absence of allegations of misuse or un-reimbursed charges or alleged problems with game consoles post-breach); *In re: Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 133 to 135 (D Me 2009), aff'd in part, rev'd in part *sub nom. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir 2011) (fraudulent charges that are reversed or reimbursed held insufficient to meet injury elements of claim for negligence, breach of contract or violation of Maine Unfair Trade Practices Act).

100 See, e.g., *Krottner*, 406 Fed. App'x 129, at *1 (9th Cir 2010) (finding '[t]he mere danger of future harm' insufficient to support a Washington common law claim of negligence); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d

receive mixed treatment.[101] Claims of injury alleging that a plaintiff 'overpaid' or 'wouldn't have shopped' for products or services later associated with a data breach have also had mixed results.[102] Claims that a plaintiff's personal information itself suffered a loss in value as a result of the breach are usually rejected as implausible.[103] Similarly, an alleged loss of ancillary benefits that may have become unavailable because of the breach is usually, though not always, deemed too speculative to survive a motion to dismiss.[104] Finally, as in other contexts, allegations of mere anxiety or emotional harm are usually held to be non-cognisable absent physical injury.[105] Even if complaints in this area thus manage to succeed in otherwise navigating the various theories for framing the causes of action asserted in a particular case, the need also to plead and show injury as an element of the causes of action continues to pose challenges in many actions.

629, 639 and 640 (7th Cir 2007) (same under Indiana law); *Alonso v. Blue Sky Resorts*, LLC, 179 F. Supp. 3d 857, 885 and 886 (SD Ind 2016) (same under Kentucky common law); Moyer, 2014 WL 3511500, at *7 (same under Illinois common law and consumer protection claim).

101 Compare *Pisciotta*, 499 F.3d at 639 (not actionable), *Welborn v. Internal Revenue Serv.*, No. 15–1352, 2016 WL 6495399, at *11 and *12 (DDC 2 Nov 2016) (same), *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 16-cv-00014, 2016 WL 6523428, at *11 (SD Cal 3 Nov 2016) (same); *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1233–34 (D Nev 2020) (same), with *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 829 and 830 (7th Cir 2018) (credit monitoring costs and 'significant' lost time held actionable under relevant state laws); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 162 (1st Cir 2011) (mitigation damages held actionable for foreseeable harms for claims under Maine law); *In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1204 and 1205 (D Or 2016) (similar for claims under Washington law); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-cv-09600, 2015 WL 3916744, at *5 (CD Cal 15 Jun 2015) (similar for claims under California law); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460 (D Md 2020) ('time and money [spent] to mitigate harms' for breach where personal information was at risk of actual or threatened harm was sufficient to establish injury-in-fact).

102 Compare *Moyer*, 2014 WL 3511500, at *7 (insufficient allegation that pricing covered added costs of data security), *Bell v. Blizzard Entm't Inc.*, No. 12-cv-09475, 2013 WL 12132044, at *8 (CD Cal 11 Jul 2013) (alleged loss of resale value unavailing where resale not available), with *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 986 (ND Cal 2016) (allegation that medical fees covered data security sufficient for 'benefit of the bargain' theory); *Sony II*, at 942, 991, 993, 1007 (allegation sufficient for omissions-based claims under California law, but not Texas or Florida law); *Grigsby v. Valve*, No. C12–0553JLR, 2013 WL 12310666, at *3 (WD Wash 18 Mar 2013) (overpayment allegation sufficient under Washington law); *In re: Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1078 and 1177 (D Minn 2014) ('overpayment' allegation rejected but 'would not have shopped' allegation accepted).

103 *Dugas*, 2016 WL 6523428, at *11 (allegation that value of PII was effective held insufficient under California statute); *Sony II*, at 994 (alleged valuing of PII unavailing under Florida law); *Burrows v. Purchasing Power, LLC*, No. 12-CV-22800, 2012 WL 9391827, at *3 (SD Fla 18 Oct 2012) (same). But see *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 865 (ND Cal 2011) (allegations of lost value sufficient for common law claim but not statutory claim).

104 See *Anderson*, 659 F.3d at 167 (lost opportunity for rewards points not actionable under Maine law). But see *In re: Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *11 (ND Ga 5 Mar 2018) (alleged loss of ancillary opportunity for earning payment card 'rewards' accepted for purposes of pleading injury).

105 *Sion v. Sunrun*, No. 16-cv-05834, 2017 WL 952953, at *2 (ND Cal 13 Mar 2017) (FCRA); *Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc.*, No. 081568, 2009 WL 799760, at *4 (ED La 24 Mar 2009) (Louisiana law).

Conclusion

The expanding scope and frequency of data breaches, in combination with the complex and changing legal landscape evidenced by the judicial decisions and statutory developments referenced in this chapter, promise to provide fertile ground for plaintiffs to continue to initiate litigation following such incidents. Companies that are subject to data breaches are accordingly well advised to engage skilled and experienced defence counsel as lawsuits ensue, especially given the significant potential exposure arising from the aggregate liability theories and procedures that plaintiffs typically seek to advance or exploit.

Appendix 1

About the Authors

Kevin Angle
Ropes & Gray LLP

Kevin Angle is counsel in the data, privacy & cybersecurity group, based in Ropes & Gray's Boston office. He represents a broad range of companies on privacy and cybersecurity matters, guiding clients through the existing patchwork of US federal and state laws as well as the European Union's comprehensive General Data Protection Regulation (GDPR) and other international privacy and cybersecurity laws. Kevin advises clients on privacy and cybersecurity matters arising in corporate transactions. He also assists clients in responding to data breach incidents, helping clients in assessing their legal obligations following a breach and in responding to regulatory authorities and others.

Richard Batchelder, Jr
Ropes & Gray LLP

Partner Richard D Batchelder, Jr has advised Ropes & Gray clients for 30 years in a wide range of high stakes litigation matters before courts throughout the country. In recent years, Richard has handled a number of significant contractual and indemnification disputes for life sciences and healthcare clients of the firm. He has advised many of the firm's private equity clients and their portfolio companies in numerous capacities, such as analysing litigation risk in proposed transactions, representing them in court post-acquisition, and in bankruptcy-related litigation. In addition, Richard actively participates in the data, privacy and cybersecurity group, helping clients respond to incidents and defending them in any related proceedings. Richard's experience in this area includes defending TJX and Target in class action lawsuits brought by financial institutions in the wake of two of the largest data breaches in US history.

Nameir Abbas
Ropes & Gray LLP

Nameir Abbas is an associate in the data, privacy and cybersecurity practice in Ropes & Gray's Washington, DC office. Nameir focuses his practice on complex data protection matters. His diverse practice includes counseling clients across a range of industries on issues relating to privacy compliance, cybersecurity preparedness, data breach response and due diligence.

Danielle Bogaards
Ropes & Gray LLP

Danielle Bogaards is an associate in the litigation and enforcement group in Ropes & Gray's San Francisco office. She focuses her practice on complex commercial litigation, government investigations and data privacy matters. Danielle's diverse practice, spanning an array of litigation and regulatory matters, includes disputes involving securities, employment, corporate governance, compliance and commercial issues. As a participant in the data, privacy and cybersecurity practice group, Danielle assists clients respond to data security incidents and counsels clients on major data privacy and security laws and regulations, including the California Consumer Privacy Act.

Anne Conroy
Ropes & Gray LLP

Anne E Conroy is an associate in Ropes & Gray's litigation and enforcement practice group in New York. Anne's practice focuses on complex commercial litigation, shareholder disputes, regulatory matters, and civil and criminal government enforcement matters. She has represented clients in matters involving securities laws, shareholder actions, and general commercial disputes.

Sara Ramsey
Ropes & Gray LLP

Sara Ramsey is an associate in the litigation and enforcement group in Ropes & Gray's San Francisco office. At the University of California, Berkeley, School of Law, Sara served as the symposium editor for the Berkeley Law Journal of Employment and Labor Law. Sara also successfully advocated for clients in the Workers' Rights Clinic and Community Economic Justice Clinic.

Ropes & Gray LLP
60 Ludgate Hill
London EC4M 7AW
United Kingdom
Tel: +44 20 3201 1500
Fax: +44 20 3201 1501
rohan.massey@ropesgray.com
edward.machin@ropesgray.com

Prudential Tower
800 Boylston Street
Boston, MA 02199
United States
Tel: +1 617 951 7000
Tel: +1 617 951 7050
richard.batchelder@ropesgray.com
kevin.angle@ropesgray.com

1211 Avenue of the Americas
New York, NY 10036-8704
United States
Tel: +1 212 596 9000
Fax: +1 212 596 9090
anne.conroy@ropesgray.com
Three Embarcadero Center
San Francisco, CA 94111-4006
Tel: +1 415 315 6300
Fax: +1 415 315 6350
danielle.bogaards@ropesgray.com
sara.ramsey@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4600
Fax: +1 202 508 4650
nameir.abbas@ropesgray.com
raffi.teperdjian@ropesgray.com

www.ropesgray.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-595-5