EMERGING ISSUES IN DATA BREACH AND PRIVACY REGULATION CLASS ACTIONS©

Steven P. Benenson & Russell L. Porter
Porzio, Bromberg & Newman, PC*

I Introduction

In a 2018 survey of over 400 general counsel, their direct reports, and chief legal officers, roughly 30% identified data privacy and security as the next significant wave of class action litigation. See The 2018 Carlton Fields Class Action Survey at 9.[1] There are two basic types of class actions at play: "data breach" and "data privacy regulation."

In the typical data breach case, a malign third party exploits a security vulnerability and steals data. Common breaches include network hacks, exposed networks, nation-state attacks, insider attacks, cyber-espionage, and lost or stolen data devices.[2] The stolen data then is used for identity fraud, held ransom, appropriated for competitive advantage, or exploited for intelligence-gathering purposes. Plaintiffs claim that the target company acted negligently, engaged in unfair business practices, fraud or misrepresentation and/or breached its contract, by

* Steven P. Benenson is a senior litigation principal with Porzio, Bromberg & Newman, PC, in New York City and Morristown, New Jersey, and chairs the firm's complex litigation practice. He has been defending class actions for over 30 years in diverse industries and businesses in state and federal trial and appellate courts across the country. He is recognized in *Best Lawyers in America*, in Mass Tort Litigation/Class Actions – Defendant, and served as the Program Chair of the 2016 ABA National Class Action Symposium. Steve is a frequent presenter and author on class action topics. Russell L. Porter is an associate in Porzio's New York City office. He represents clients in commercial, products liability, environmental tort and other cases in New York state and federal courts.

[1] "Companies cite the potential for data breach claims associated with internet connected products, such as medical devices and home appliances, as an example of the predicted next wave of data breach litigation." Id.

[2] Former FBI Director Robert Mueller, III famously observed that there were two categories of companies: those that have been breached, and those that will be. (Comments made at RSA Cybersecurity Conference in March 2012). See https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

failing to take reasonable measures to secure personal identifying information ("PII"),[3] respond promptly to system breaches, and provide timely notification to protect against identity theft and associated losses.

In contrast, data privacy regulation cases do not necessarily involve a third-party theft nor are they based on tort or contract claims. Instead, data privacy claims are based on mere *technical* violations of consumer protection regulations governing the collection, handling and use of PII.

Depending on the type of case, plaintiffs may include consumers, insureds, employees, business partners, and financial service firms. The damages and other equitable relief obtained[4] can be substantial, as can awards of attorneys' fees under consumer protection statutes.[5] Courts are still grappling with how to deal with the resulting lawsuits. We highlight some of the emerging issues in the federal cases involving jurisdiction, mandatory arbitration provisions, pleading sufficiency, discovery privileges, class certification and settlement.[6]

[3] PII includes social security numbers, credit or debit account numbers, passports, driver's licenses, dates of birth, passwords, biometric data, medical records, email addresses etc.

[4] This often includes the costs of replacing credit and debit cards, late or overdraft fees, credit reports and insurance, credit monitoring services fees, and miscellaneous identity theft expenses for classes with millions of members.

[5] For example, in what is still the largest data breach in history, Yahoo agreed to pay $50 million to a class of some 3 billion account holders, plus $35 million in attorneys' fees and expenses. In re Yahoo Inc. Customer Data Security Breach Litigation, Civil Action No. 5:16-02752 (N.D. Cal. Oct. 22, 2018). Health insurer Anthem Inc. paid $115 million to settle a class action after a data breach exposed the PII of over 78 million people. In Re Anthem, Inc. Data Breach Litigation, Civil Action No. 5:15-02617 (N.D. Cal. Aug. 15, 2018). Target agreed to a $10 million settlement in a data breach affecting 70 million customers, plus $6.75 million in attorneys' fees and expenses. In re Target Corp. Customer Data Security Breach Litigation, MDL No. 14-2522 (D. Minn. March 19, 2015). GameStop agreed to pay up to $235 of expenses for each of 1.3 million credit card holders, plus class counsel fees and costs of $557,500, after a breach of its servers resulted in the theft of PII. Bray v. GameStop, Civil Action No. 1:17-01365 (D. Del. July 23, 2018). And Wendy's entered into a $3.4 million settlement in which affected customers could collect up to $5,000 in compensation. Torres, et al. v. Wendy's International LLC, Civil Action No. 6:16- 210 (M.D. Fla. Aug. 23, 2018).

[6] The Class Action Fairness Act of 2005 ("CAFA") expanded federal jurisdiction over class actions by granting district courts original jurisdiction over putative class actions in which minimal (rather than complete) diversity exists and the amount in controversy exceeds $5 million. *See* 28 U.S.C. § 1332(d)(2). CAFA defines "class action"

II. Standing in Data Breach Class Actions

A. The Injury-In-Fact Requirement and the Risk of Future Identity Theft

Article III, §2 of the United States Constitution limits the jurisdiction of the federal courts to actual "cases" or "controversies." This "bedrock requirement," Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 471 (1982), restricts the province of the judiciary to "decid[ing] on the rights of individuals." Marbury v. Madison, 5 U.S. (1 Cranch) 137, 170 (1803). A plaintiff seeking redress in federal court must therefore have standing to sue. Ballentine v. United States, 486 F.3d 806, 810 (3d Cir. 2007). Standing exists when a plaintiff suffers an injury-in-fact that is causally connected to the defendant's wrongful conduct, which can be remedied by a decision in the plaintiff's favor. Lujan v. Defs. of Wildlife, 112 S. Ct. 2130, 2136 (1992). Courts have held that the mere potential for future injury will not suffice and that harm complained of must be "actual or imminent, not conjectural or hypothetical." Id.

In the typical data breach class action, the plaintiffs may have been reimbursed for any fraudulent charges, and offered free credit monitoring services. Plaintiffs nonetheless assert that the PII theft subjects them to an increased *risk* for future identity theft, causing emotional harm and forcing them to incur additional mitigation costs. Defendants often seek dismissal under Fed. R. Civ Pro. 12(b)(1) arguing that such a non-imminent potential for future harm does not constitute an injury-in-fact. This frequently litigated issue has led to a circuit split.

Some courts have taken a narrow view of the issue. For example, in Reilly v. Ceridian, 664 F. 3d 38 (3d Cir. 2011), employees filed a putative class action after the defendant-payroll processing vendor's computer system was breached and hackers extracted PII for over 25,000

as "any civil action filed under [Federal Rule of Civil Procedure 23] or similar State statute or rule . . . ." *Id*. at (d)(1)(B).

individuals. Id. at 40. Plaintiffs alleged that the defendant was negligent in safeguarding their PII, but they were unaware whether the stolen data had been used. Id. The district court granted the defendant's motion to dismiss, finding that the plaintiffs did not suffer the requisite injury-in-fact. Id. at 41. The Third Circuit affirmed. Id. at 46.

Other courts have been more receptive to these claims. In Pisciotta v. Old National Bancorp., 499 F. 3d 629 (7th Cir. 2007), the Seventh Circuit found that the plaintiffs had standing when faced with operative facts similar to those in Reilly. The Pisciotta plaintiffs were victims of a bank website's breach and claimed standing based on the risk of future misuse of their PII with no evidence of financial loss. Id. at 631-632. The court found that standing existed: "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent defendant's actions." Id. at 634.

B. The Supreme Court's Clapper Decision and its Fallout

The diametrically opposed holdings in Reilly and Pisciotta created significant uncertainty that commentators thought would be clarified when the Supreme Court granted certiorari in Clapper v. Amnesty Intern., USA. 133 S. Ct. 1138 (2013). Clapper did not involve a classic data breach scenario. The plaintiffs were American citizens whose employment involved communicating with likely subjects of Foreign Intelligence Surveillance Act surveillance. Id. at 1142. The plaintiffs complained that their own communications could be subjected to the same surveillance. Id. They asserted, and the Second Circuit agreed, that there was an injury-in-fact based upon the "objectively reasonable likelihood that their communications will be acquired…at some point in the future." Id. at 1143, 1146. The Supreme Court disagreed, finding that the plaintiffs' "theory of *future* injury is too speculative to satisfy the well-

established requirement that threatened injury must be certainly impending." Id. at 1143. The majority's decision, however, contained an important footnote noting that it was possible to "find standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." Id. at fn 5.

Perhaps not surprisingly, post-Clapper cases have continued to yield inconsistent results with a moderate trend in favor of finding standing. For example, in 2015, the Seventh Circuit in Remijas v. Neiman Marcus Group, LLC, 794 F. 3d 688 (7th Cir. 2015), reversed after a district court dismissed a data breach suit relying in part on Clapper. The Remijas plaintiffs had their credit card numbers stolen by hackers who breached Neiman Marcus' network. Id. at 690. Approximately 9,000 of the 350,000 affected customers had experienced instances of fraud. Id. at 694. The other plaintiffs asserted that the increased risk of future misuse of their data and the cost associated with mitigating it met the injury-in-fact requirement. Id. at 694-695.

The Seventh Circuit found these injuries to be sufficient, noting that "Clapper does not…foreclose any use whatsoever of future injuries to support Article III standing." Id. at 693. The court then relied on the footnote in Clapper and held:

> [I]t is plausible to infer that the plaintiffs have shown substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.

Id. at 693-694.

On this basis, the Seventh Circuit concluded that the "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing." Id. at 693.

In 2016, the Sixth Circuit reached a similar conclusion in Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384 (6th Cir. 2016). There, the court found standing for plaintiffs whose PII had been exposed when an insurance carriers' network was breached noting that, "Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for…fraudulent purposes." Id. at 388. The Galaria court concluded this absent any allegation that the stolen PII had been misused. Id. at 386-387.

In 2017, however, the Fourth Circuit in Beck v. McDonald, 848 F. 3d 262 (4th Cir. 2017), affirmed the dismissal of a very similar suit. The Beck plaintiffs complained of an increased risk of future identity theft and associated costs when a laptop containing their PII was stolen from a healthcare provider. Id. at 2267. The Fourth Circuit found the plaintiffs lacked standing stating, "for the Plaintiffs to suffer the harm of identity theft that they fear, we must engage with the same attenuated chain of possibilities rejected by the Court in *Clapper*." Id. at 275. This skeptical stance has been adopted by other courts. See Whalen v. Michaels Stores Inc., 689 Fed. Appx. 89 (2d Cir. 2017) (plaintiff whose credit card number was stolen as part of a data breach lacked standing where fraudulent charges were reimbursed and no other PII was exposed).

In Attias v. Carefirst, Inc., the D.C. Circuit reviewed the dismissal of a suit brought by victims of a health insurer's data breach. 865 F. 3d 620 (D.C. Cir. 2017). The district court had dismissed the case for lack of standing, finding that the increased risk of future identity theft too speculative to be an injury-in-fact. Id. at 622-623. There were no allegations that the data had actually been used to the plaintiffs' detriment. Id.

But the D.C. Circuit reversed, holding:

> No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.

Id. at 629.

Defendants petitioned the Supreme Court for certiorari. Many practitioners saw this as an ideal opportunity for the Court to resolve the issue and provide useful guidance for future cases. On February 20, 2018, to the surprise of many, the Supreme Court declined to grant certiorari leaving the D.C. Circuit's decision in place. See Carefirst, Inc. v. Attias, 138 S. Ct. 981 (2018). The Court's denial of certiorari is not precedential, and does not indicate how it will ultimately tackle the circuit conflict. Until then, confusion and non-uniform results will continue and data breach plaintiffs have several friendly circuits that will likely allow their cases to proceed past a motion to dismiss on standing.

III. Standing in Data Privacy Regulation Class Actions

The collection, use and storage of biometric data PII such as fingerprints, facial geometry and iris scans have been fertile grounds for data privacy regulation class actions under the Illinois Biometric Information Privacy Act ("BIPA"). Passed in 2008, BIPA was the first statute to simultaneously regulate biometric data, and afford a private cause of action for violations of its rules. At its heart, BIPA requires companies to obtain written consent before collecting biometric PII and to securely store it once obtained. See 740 I.L.C.S. 14/1 et seq.[7] BIPA's enactment triggered a wave of data privacy class actions.

[7] As of November 2018, Texas and Washington have enacted similar laws, but they do not create a right to a private cause of action for violations. The recently enacted California Consumer Privacy Act provides a private right of action where companies fail to implement a general privacy policy or otherwise disclose what PII has been collected, and from where, for what use, and whether it will be disclosed or sold and to whom, and the right to opt out or to have the data deleted without penalty.

Just like their data breach counterparts, plaintiffs in BIPA cases are often hard pressed to demonstrate any pecuniary loss. Defendants therefore regularly argue that the absence of out-of-pocket loss means that no injury-in-fact exists. Motions based on these arguments have met with mixed results.

Although not a data privacy case, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016), was initially viewed as a death-knell for the majority of BIPA-related suits. Spokeo operates a website allowing users to find information about a person's "occupation, hobbies, finances, shopping habits, and musical preferences". Id. at 1546. Plaintiff learned his website profile contained inaccurate information regarding his socioeconomic status. Id. at 1544. He alleged this violated the Fair Credit Reporting Act of 1970, but could not point to any concrete harm suffered because of these inaccuracies. Id. at 1544, 1549-1550.

The Supreme Court held that "a bare procedural violation, divorced from any concrete harm" could not satisfy the injury-in-fact requirement. Id. at 1549. Although many expected this statement would curtail BIPA-related filings, the Court also noted that "this does not mean…that the risk of real harm cannot satisfy the requirement of concreteness." Id. This equivocal language, like that in Clapper's footnote, has resulted in varied rulings similar to those rendered in the data breach arena.

For instance, in McCollough v. Smarte Carte, Inc., 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016), a public locker provider collected customers' fingerprints to use as keys without obtaining written consent. Id. at *1. This practice violated BIPA, but the plaintiffs could allege no concrete damages and voluntarily provided their fingerprints to the defendant. Id. at *2-3. The court dismissed the case finding this mere "technical violation" of BIPA, without more, did not constitute a sufficient injury-in-fact under Spokeo. Id. at *4-5.

The Second Circuit followed suit when it affirmed dismissal in Santana v. Take-Two Interactive Software, Inc., 717 Fed. Appx. 12 (2d Cir. 2017). Plaintiffs voluntarily provided the defendant-video game publisher with facial biometric PII to create personalized in-game characters. Id. at 14. Similar to McCollough, the defendant failed to obtain written consent and committed technical BIPA violations, but the plaintiffs had suffered no out-of-pocket loss. Id. The Second Circuit observed that BIPA's core objective is to "prevent the unauthorized use, collection, or disclosure of an individual's biometric data." Id. at 15. The court reasoned that dismissal was warranted because the BIPA violations were technical and implicated no risk that biometric data would be misused. Id. at. 15-17.

Potential defendants took comfort in the McCollough and Santana decisions. It seemed that the tide of BIPA class action litigations would be stemmed by the requirement that plaintiffs demonstrate harm beyond a mechanical violation of the statute. Recent developments suggest this sense of security may have been misplaced.

In February 2018, the Northern District of California allowed a BIPA suit to proceed against Facebook without showing financial injury. Patel v. Facebook, Inc., 290 F. Supp. 3d 948 (N.D. Cal. 2018) involved a Facebook feature that uses facial geometry to identify individuals in user-uploaded photographs and then suggest this person be "tagged" for identification and profile-linking purposes. Id. at 951. Unlike McCollough and Santana, some of the Patel plaintiffs were not necessarily aware that their information was being collected. Id.
There was no financial or other tangible harm. But the court found that the plaintiffs had suffered the requisite injury-in-fact, stating:

> [T]he plain text of BIPA…leave(s) little question that the Illinois legislature codified a right of privacy in personal biometric information. There is equally little doubt about the legislature's

> judgment that a violation of BIPA's procedures would cause actual and concrete harm. BIPA vested in Illinois residents the right to control their biometric information by requiring notice before collection and giving residents the power to say no by withholding consent…Consequently, the abrogation of procedural rights mandated by BIPA necessarily amounts to a concrete injury.

Id. at 953-954.

Patel may appear in line with McCollough and Santana because plaintiffs did not voluntarily submit their biometric PII to Facebook. Some plaintiffs posted photographs from which Facebook extracted their facial geometry while others had their information taken from photographs posted by third-parties. The court's opinion, however, did not limit its findings to the latter class of plaintiffs. Patel may portend a data privacy circuit split similar to that in data breach cases.[8]

IV. Class Action Waiver and Arbitration Provisions

In addition to standing challenges, class action waiver and arbitration provisions in contractual terms of use and other agreements present a formidable obstacle to pursuing data breach or data privacy regulation class actions. Since the Supreme Court's decision in AT&T Mobility, LLC v. Concepcion, 131 S. Ct. 1740 (2011), which validated the inclusion of class action waiver and mandatory arbitration provisions in consumer contracts, many companies have included them. Such clauses have been invoked in data breach cases, and have withstood attacks asserting that they are procedurally unconscionable under state law, an issue left open by Concepcion.

For example, in Flores v. Uber Technologies, Civil Action, No. 17-cv-8503 (C.D. Cal. Sept. 5, 2018), both users and drivers of the popular car service Uber sued after a breach exposed

[8] Defendants that unsuccessfully move for dismissal on the basis of standing have sometimes obtained summary judgment on identical grounds after conducting damage-related discovery. See, e.g. Walker v. Boston Med. Ctr., 2015 WL 9946193 (Mass. Super. Ct., Nov. 20, 2015).

PII for millions of people. Uber's terms and conditions contained a conspicuously displayed arbitration and class action waiver clause. Id. at *2. Uber moved to compel arbitration under this and related provisions in its terms of service. Id. at *4. Plaintiffs argued their claims fell outside the arbitration clause's scope, and the provisions were unconscionable and insufficiently prominent. Id. at *6.

The court first noted that the "principal purpose of the FAA [Federal Arbitration Act] is to ensure that private arbitration agreements are enforced according to their terms." Id. at *3. As such, the court's involvement is limited to "determining (1) whether a valid agreement to arbitrate exists and, if it does, (2) whether the agreement encompasses the dispute at issue." Id. at *4. If the answers to these questions are in the affirmative, section 4 of the FAA requires courts to compel arbitration under the terms of the agreement. Id. The court found that the arbitration and class action waiver clauses were clear, unambiguous and compelled the parties to submit the dispute to arbitration. Id. at *6-7.

V. Failure to State a Claim

Data breach claims that sound in common law negligence and breach of contract may also be vulnerable to substantive (rather than jurisdictional) dismissal under Fed. R. Civ. Pro 12(b)(6) because the pleadings do not plausibly meet the proximate causation requirement absent allegations of clear financial injury. See Bell Atlantic Corp. v. Twombly, 127 S. Ct. 1955 (2007) and Ashcroft v. Iqbal, 129 S. Ct. 1937 (2009).

In In re SuperValu, Inc. Customer Data Security Breach Litigation, 2018 WL 1189327 (D. Minn. Mar. 7, 2018), hackers stole customer credit card information from a grocery store's payment-processing network. Sixteen plaintiffs sued, but only one had experienced fraudulent charges and these charges were reimbursed. Id. at *1-2. The remaining plaintiffs sought

damages relating to the increased risk of future identity theft. Id. at *2. The district court initially dismissed the entire suit, finding there was no injury-in-fact for any plaintiff. Id. The Eighth Circuit affirmed on the fifteen plaintiffs who had not experienced fraudulent charges, but reversed on the other plaintiff finding that he satisfied the injury-in-fact requirement because he had experienced fraudulent charges. Id. at *3-4. The case was remanded for consideration of whether his allegations otherwise stated a claim upon which relief could be granted. Id.

On remand, the district court dismissed the case for failing to state a claim because there were no cognizable damages. Specifically, the court found that applicable state law negligence claims required allegations of out-of-pocket financial losses. Id. at *12-13. The plaintiff's inability to alleged such damages proved fatal. Id.

In In re Sony Gaming Networks and Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942 (S.D. Cal. 2012), the district court found that the plaintiffs sustained an injury-in-fact under Article III , but dismissed the case for failing to allege a cognizable injury under California state law. The plaintiffs were consumers whose PII was stolen when the defendant's network was breached. Id. at 950-951. No out-of-pocket losses were alleged, but the plaintiffs claimed that the wrongful dissemination of their PII alone would meet the injury-in-fact requirement. Id. at 957. The court agreed, stating this "future harm may be regarded as a cognizable loss sufficient to satisfy Article III's injury-in-fact requirement." Id. at 958.

The court next considered the defendant's motion to dismiss for failure to state a cognizable negligence claim under California state law. The court noted that "[u]nder California law, appreciable, nonspeculative, present harm is an essential element of a negligence cause of action." Id. at 962. As the plaintiffs had only alleged potential future harm, the court dismissed their common law negligence claim:

> While Plaintiffs have currently alleged enough to assert Article III standing to sue based on an increased risk of future harm, the Court finds such allegations insufficient to sustain a negligence claim under California law….Accordingly, without specific factual statements that Plaintiffs' Personal Information has been misused, in the form of an open bank account, or un-reimbursed charges, the mere danger of future harm, unaccompanied by present damage, will not support a negligence action.

Id at 963.

These rulings suggest that defendants faced with common law negligence claims should consider motions to dismiss absent clearly pled damages. Such motions can be effective in obtaining either complete dismissals or narrowing the class of plaintiffs and issues remaining for discovery.

VI. Discovery and Privilege Issues

In discovery, plaintiffs often seek internal investigative documents relating to how and when a breach occurred and what steps the target company took in response. Such requests may implicate the attorney-client[9] or work-product privileges.[10] Courts faced with these questions engage in a fact-specific analysis that turns on when counsel was hired, the level of their involvement and the purpose behind the sought-after materials' creation.

For example, in In re Experian Data Breach Litigation, 2017 WL 4325583 (C.D. Cal. May 18, 2017), the court denied a motion to compel a report prepared by a forensic consultant hired to investigate a data breach. After Experian discovered the breach, it immediately retained

[9] The attorney-client privilege protects confidential attorney-client disclosures that relate to the subject of a legal representation or assistance. Fisher v. United States, 96 S. Ct. 1569, 15677 (1976). The privilege extends to communications made by corporate employees to attorneys providing counsel to the corporation itself, Upjohn v. United States, 101 S. Ct. 677, 685 (1981), and attorneys and experts or consultants hired to assist in the provision of legal services to the company. United States v. Kovel, 296 F.2d 918, 921 (2d Cir. 1961).

[10] The work-product doctrine shields materials prepared in anticipation of litigation or trial by or for a party or its representative, except where the requesting party can demonstrate a significant need for the materials and cannot obtain them without undue hardship. See Fed. R. Civ. P. 26(b)(3).

outside counsel to advise as to its response before litigation was commenced. Id. at *2. Outside counsel then engaged a third-party forensic consultant to prepare a report analyzing what had transpired. Id. The consultant provided the report to Experian's outside counsel, who then shared it with the company's in-house attorneys to develop their legal strategy in response to the foreseeable class action. Id.

The plaintiffs sought production of that report, arguing that Experian had "independent business duties to investigate" the data breach and hired the consultant to fulfill them. Id. Experian contended that the report was work-product material prepared by a third-party retained by outside counsel to provide legal advice. Id. The court sought to determine if the report was prepared because of litigation by weighing factors such as the timing of retention of the non-testifying expert, and the existence of other evidence, including supporting affidavits and engagement letters. Id.

The court noted that the consultant was hired by Experian's outside counsel to "assist…in providing legal advice in anticipation of litigation". Id. The court was not swayed by the consultant's having done unrelated work for Experian directly. Id. at *3. The court also found that the work-product doctrine's hardship exception did not apply because the plaintiffs could obtain the same data that the consultant relied upon directly from Experian in discovery. Id. Finally, the court noted that work-product protection was not waived by sharing the report with Experian's customer, T-Mobile, because the disclosures were "very limited and closely controlled" by Experian's outside and in-house attorneys. Id. The fact that Experian and T-Mobile had signed a joint defense agreement before the report was shared weighed against finding a waiver. Id.

A more nuanced result followed in In re Premera Blue Cross Customer Data Security Breach Litigation, 296 F. Supp. 3d 1230 (D. Oregon, Oct. 27, 2017). There, the plaintiffs moved to compel the production of: (1) documents prepared by the defendant's employees that incorporated the advice of counsel, but were not prepared by or sent to counsel ("Category One"); (2) documents that were prepared at the request of counsel, but not prepared by or sent to counsel and which did not appear to be prepared because of the litigation ("Category Two"); and (3) documents relating to an outside forensic consultant's investigation of the security event that triggered the litigation ("Category Three"). Id. at 1240-1245.

Regarding Category One, the court concluded that the entirety of these documents were "not internal factual investigatory reports prepared at the request" of an attorney. Id. at 1241. Instead, they included "business documents that the company would have prepared regardless of litigation" and were not attorney-client or work-product privileged. Id. at 1241-1242. The court noted, however, that certain of these documents contained attorney-client protected materials such as drafts, edits and "redlines by an attorney communicating legal advice." Id. at 1242. These documents were held immune from production under both the attorney-client privilege and work-product doctrine. Id.

Category Two consisted largely of documents prepared at the request of attorneys relating to technical aspects of the breach, company policies and public relations concerns. Id. The court again noted the primary purpose of the majority of those documents "was not to communicate with counsel or obtain legal advice, but instead to perform a business function." Id. While some of these business functions were delegated and managed by outside counsel, this did not render the documents attorney-client privileged. Id. As to work product, the defendant argued that these documents had a dual business and legal purpose. Id. at 1244. The court

concluded that the defendant had failed to show that "the documents were created because of litigation rather than for business reasons, or that the documents would not have been created in substantially similar form but for the prospect of litigation" and compelled their production. Id.

The court found that the Category 3 reports generated by the defendant's outside forensic consultant were discoverable because the defendant retained and directed the consultant rather than its attorneys. Id. at 1245. Even though "the supervisory responsibility later shifted to outside counsel, the scope of the work performed did not change." Id. The court reasoned this "is not sufficient to render all of the later communications and underlying documents privileged or immune from discovery as work product." Id.

These cases strongly suggest that once a company learns of a data breach, it should promptly retain outside counsel as a "breach coach," who will then lead the investigation and response process and have complete control over the retention and direction of any outside consultants, and their work product.

VII. Class Certification Issues

A. Predominance Issues

Cybersecurity plaintiffs most commonly seek certification under the predominance prong of Fed. R. Civ. Pro. 23(b)(3) and can usually satisfy the numerosity, commonality, typicality and adequacy requirements of Rule 23(a). Although there is limited case law on the subject, several reported decisions illustrate that plaintiffs can have trouble meeting the predominance requirement because the nature of the injuries suffered by members of the putative class often varies.

For instance, in In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 293 F.R.D 21 (D. Me. 2013), the court denied class certification because it was not convinced that common

damage questions predominated. There, a putative class of grocery store customers sued when their credit card information was stolen by hackers. Id. at *23. After years of litigation, the proposed class consisted of customers who made out-of-pocket payments to mitigate the risk of fraud and certification was sought under Rule 23(b)(3). Id. at *24. The court concluded that the plaintiffs had met the prerequisites of Rule 23(a). Id. at *24-30.

Turning to predominance under Rule 23(b)(3), the court noted that although there were common liability questions regarding whether the defendant adequately secured customer PII, "things differ…in the actual impact on particular cardholders…and the actual mitigating steps they took and the costs they incurred." Id. at *30. The plaintiffs argued that damages could be demonstrated for the entire class through statistical proof presented by experts who would testify as to what proportion of the fees incurred were attributable to the intrusion as opposed to other causes. Id at *31-32. This would enable the jury to render a lump sum verdict that would then be divided amongst the class. Id.

The court acknowledged that certification had been granted in non-data breach cases where expert witnesses opined that damages could be calculated and distributed to class members using a statistical formula. Id. at *32-33. The Hannaford plaintiffs had failed to offer such an expert opinion with their certification motion and the court held this failure, coupled with the inherent damages-related predominance issues, required denial of certification. Id. at *33.

Contrasted with In re Hannaford, a group of financial institutions that had to replace customer credit/debit cards, reimburse fraudulent charges and take other remedial steps in response to the data breach at nation-wide Target stores obtained class certification in In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482 (D. Minn. 2015). Target

opposed the application, arguing that damages had to be calculated on a bank-by-bank basis "meaning that individual damages issues predominate over any potential class-wide issues." Id. at *486. The court disagreed, and noted that the plaintiffs had offered expert testimony on the issue:

> Although Plaintiffs' damages may ultimately require some individualized proof, at this stage Plaintiffs have established, through Dr. Cantor's report, that it is possible to prove classwide common injury and to reliably compute classwide damages resulting from reissuance costs and fraud losses.

Id. at *489.

Although In re Hannaford and In re Target Corp. highlight the importance of expert statistical testimony to prove class-wide damages, certification may also turn on the similarity between the injuries suffered by members of the putative class and the ease with which a lump sum verdict can be rendered and then divided amongst them. The In re Hannaford plaintiffs were individual customers who likely behaved differently when their PII was compromised. Conversely, the financial institutions who sued in In re Target Corp. suffered an essentially identical type of injury all readily attributable to the network breach. This most likely explains the disparate results reached.

B. Decertification Due to Adequacy and Conflicts of Interest

Adequacy issues due to conflicts of interest between data breach plaintiffs have resulted in decertification at the settlement approval stage.[11] In Remijas v. Neiman Marcus Group, LLC, 2018 WL 4404673 (N.D. Ill., Sept. 17, 2018), the district court decertified the class when the parties requested approval of a proposed settlement. After the 7th Circuit found the plaintiffs had

[11] The "Rule 23 adequacy inquiry…uncovers conflicts of interest between the named plaintiffs and the class they seek to represent." Langbecker v. Ele. Data Sys. Corp., 476 F. 3d 299, 314 (5th Cir. 2007). Courts have noted that adequacy is the single most important factor in determining whether to certify a settlement class. See In re Prudential Ins. Co. Am. Sales Practice Litig. Agent Actions, 148 F. 3d 283, 308 (3d Cir. 1998).

standing, 794 F. 3d 688 (7th Cir. 2015), the case proceeded and a motion to simultaneously certify the class and approve the settlement was eventually filed. Id. at *2.

The case was filed after Neiman Marcus' point of sale terminals were infected with malware in some stores. Id. at *1. Three subclasses were proposed: (1) plaintiffs who made purchases at locations where the malware was present ("Subclass One"); (2) plaintiffs who made purchases at stores where no malware was installed, but during the period where the malware was present elsewhere ("Subclass Two"); and (3) plaintiffs who made purchases when no malware existed at any store ("Subclass Three"). Id. at *3. The proposed settlement contemplated financial compensation for Subclass One only and identity theft mitigation services for the others. Id.

Objectors argued that the conflict between the interests of the three subclasses and the representative plaintiffs (who were to receive $2,500) rendered them inadequate under Rule 23(a)(4). Id. at *2-3. Plaintiffs' counsel claimed this could be addressed by structuring the settlement so individual class members would not learn whether their card number had been compromised until after they had opted into the settlement. Id. at *3. The court noted this proposal created "an appearance of manipulation or dishonesty" that undermined "the integrity of the class action mechanism", but ultimately concluded that Subclass One could adequately protect the interests of Subclass Two through such a mechanism. Id.

The court, however, disagreed regarding Subclass Three. When the settlement was reached, the period in which the malware was present was public knowledge. Id. at *4. The class representatives were aware from the outset Subclass Three could "not have made their purchases at a time when the malware was active" and had little incentive to accept the proposed settlement, which afforded them no meaningful relief. Id. In fact, Neiman Marcus had offered

identity theft mitigation services before the litigation was commenced. Id. at *5. The court held that "the settlement class as it is currently composed has a fundamental conflict that undermines the adequacy of the representation of the class." Id. at *4.

Remijas demonstrates the problems that can arise when the representative plaintiffs' interests diverge from those of other class members, especially those in subclasses who will receive different remedies.

VIII. Settlement Considerations

Settlements of data breach and privacy class actions have spawned additional litigation where defense counsel and third-party administrators have not taken appropriate measures to protect against further disclosure of PII. In Beckett v. Aetna, Inc. et. als., Civil Action No. 2:17-CV-3864 (E.D. Penn. Oct. 16, 2018), defendant had settled an earlier litigation involving a discriminatory policy that required members to obtain HIV-related medications through mail order pharmacies, without the ability to speak to a pharmacist. This created an enhanced risk of exposing their HIV status. In administrating the settlement, Aetna improperly disclosed members' HIV status to legal counsel, a settlement administrator and a mailing vendor and further exposed the members' status, including their medications, by mailing claims notification letters in envelopes with clear windows.

A second lawsuit ensued. The complaint alleged that Aetna was responsible for all financial and non-financial harm caused by the disclosure under various theories of liability including negligence, negligence per se, invasion of privacy, unjust enrichment, and violations of Pennsylvania's Confidentiality of HIV Related Information Act, 35 P.S. § 7601 and Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-201-1 –201-9.3. The case was quickly mediated and settled for roughly $17 million. In addition to providing monetary relief and class

counsel's fees and expenses,[12] the settlement agreement dictates several measures designed to avoid further improper disclosures of PII:

- Use of an opaque envelope of appropriate and sufficient stock and with no transparent window so as to obscure the contents.
- Use of a return address on the outside of the envelope with no identifying information other than a P.O. box, city, state and ZIP Code;
- Including a statement on the front of the envelope that it contains "Confidential Legal Information – To Be Opened Only By The Addressee";
- Use of a protective cover page that folds around the Notice of Class Action Settlement and identifies that the information therein is confidential and solely for reading by the Settlement Class Member; and
- Use paper stock that will protect the confidentiality of the contents of the envelope from being read through the envelope.

Beckett provides useful guidance and precautions to follow when administering a data breach or privacy regulation class action settlement to avoid further unintended exposure of members' PII.

VIII. Conclusion

With the growing numbers of company data breaches—including the recent reported hack of Marriott's worldwide reservation systems—and more states considering or enacting data privacy regulations that provide a private cause of action, the jurisprudence in this fast moving area will likely continue to evolve. Efforts of companies to moot the class by quickly offering credit monitoring and fraud mitigation services, the inability of the majority of class members to allege concrete harm, the increasing use of class action waiver and arbitration clauses, and potential conflicts amongst class members pose substantial, but not insurmountable challenges in

[12] Aetna agreed to pay $500 to each of the approximately 11,875 class members who were mailed the exposed letter and $75 each to an additional 1,600 individuals whose health information was disclosed to Aetna legal counsel and the mailing vendor. In addition, class members are eligible to receive up to an additional $20,000, for financial and nonfinancial harm, upon the submission of documentation evidencing out-of-pocket expenses, and a questionnaire detailing the emotional and psychological harm they have suffered.

prosecuting these claims. Where classes have been certified and cases settled, additional care must be taken to assure that the claims administration process does not cause further disclosure of PII.