Friday, September 14, 2018

Litigation Section Breakfast Meeting

Litigation of Our Times-The Specialty Trial Series: Data Breach Litigation & Trial

Speakers:

Cari K. Dawson, Alston & Bird LLP
Michael L. McGlamry, Pope McGlamry
Phyllis B. Sumner, King & Spalding
J. Cameron Tribble, Barnes Law Group

Moderator: E. Tyron Brown, Hawkins Parnell Thackston & Young

1 CLE hour, including trial credit

Data Breach Litigation and Trial

E. Tyron Brown
Hawkins Parnell Thackston & Young LLP
Atlanta, Georgia 30308

I. WHAT IS DATA BREACH?

38 U.S. Code § 5727(4) states: "The term 'data breach' means the loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."

Additionally, the U. S. Department of Homeland Security and Department of Energy defines cyber security risk as:

> risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information, IT [Information Technology] and/or OT [Operations Technology]. Cyber security risk is one component of the overall business risk environment and feeds into an organization's enterprise risk management strategy and program. Cyber security risk cannot be completely eliminated, but it can be managed through informed decision-making processes.

The duty to protect information that is collected, stored and used by companies is associated with personally identifiable information (PII), personal health information (PHI) and personal financial information (PFI).

For most individuals, the main concern with a data breach is identity theft which can allow a thief to steal money from the individual's banking, saving and retirement accounts and to charge purchases using the individual's credit information. That, however, can be only the beginning of problems persons may suffer as a result of a data breach.

A cyber-attack and data breach can disrupt the lives of affected persons and alter the course of a company in unimaginable ways. Losses may include data loss and restoration expenses, notification costs and credit monitoring services, IT/forensic services and expenses, lost income, lost productivity, business interruption expenses, crisis management and public relations expenses, criminal extortion, theft and fraudulent transfers. Losses arising out of a data breach can include privacy and network liability, regulatory liability, media liability and technology errors and omissions.

II. HISTORY OF DATA BREACH

High profile data breaches have received tremendous attention in recent years as most individuals, businesses and governments use digital data. Since sensitive personal and business data are stored on computers, databases and cloud servers, breaching a person's data is just a matter of gaining access to restricted networks.

Data breaches, however, are not new. They have occurred since persons have kept records and private information. Before common-day digitalization of information, a thief would have to view and/or steal paper documents or find sensitive documents.

When computing and digitalization became widespread, that made it easier for criminals to steal data. Publicly-disclosed data breaches increased in frequency in the 1980s, and in the 1990s and early 2000s, public awareness of the potential for data breaches increased.

Most information on data breaches focuses on 2005 to the present. 2005 is the year of the first data breach to compromise more than 1 million records (DSW Shoe Warehouse in March 2005; 1.4 million credit card numbers and names on those accounts). It was also the year of the first data breach affecting a college (George

Mason University in January 2005; names, pictures and Social Security numbers of 32,000 students and staff). Then, in June 2005 hackers exposed 40 million credit card accounts from payment card processor CardSystems Solutions.

Now, a data breach can impact multiple millions of individuals and records.

III. RISE AND EXPANSION OF DATA BREACHES

Most of the largest data breaches have happened since 2005 as hackers became more sophisticated and entities put more data on servers and/or the cloud. The number of data breaches and records exposed in the United States since 2005 is on an upward trend. In 2005, 157 data breaches were reported, with 66.9 million records exposed. In 2014, 783 data breaches were reported, with at least 85.61 million records exposed - an increase of nearly 500 percent over 2005.

The trend has not been a consistently uphill slope. In 2009, the number of data breaches reported in the U.S. dropped to 498, from 656 in 2008. The number of records exposed, however, increased from 35.7 million in 2008 to 222.5 million in 2009.

There was also a decline in the number of data breaches reported between 2010 and 2011, with 662 data breaches reported in 2010 and 419 data breaches reported in 2011. Since 2011, however, the number of data breaches reported in the U.S. has risen steadily:

- 447 data breaches reported in 2012
- 614 data breaches reported in 2013
- 783 data breaches reported in 2014

IV. STATE, FEDERAL AND INTERNATIONAL NOTIFICATION REQUIREMENTS

A. STATE NOTIFICATION LAWS

Every state and the District of Columbia has a data breach notification law that requires businesses to notify affected individuals when their information has been compromised. There are, however, differences in the states' notification laws. Some states have a broad definition of personal information, while other states have a well-defined definition of personal information. Some states require notification if customer data has been accessed, while others require notification when there's a risk of harm. Also, the laws vary based on the type of data compromised.

The reporting requirements may cover only residents - or all affected individuals. Businesses may also be required to notify regulatory agencies, the state attorney general or consumer credit reporting agencies in the event of a breach, and the requirements may be triggered by the number of affected individuals. While most states only require these notifications happen as expediently as possible or without unreasonable delay, some states require the notifications happen within a set number of days after the breach is discovered.

The following states require businesses to notify all affected individuals, regardless of whether the individuals are residents of the state: Alabama, Arizona, Hawaii, Iowa, Mississippi, New Hampshire, North Carolina, Oregon, Texas, Vermont, and Wisconsin. The rest of the states and the District of Columbia require businesses to notify only those affected individuals who are residents of that state.

The majority of states only require notifications to be given as expeditiously as possible or without any unreasonable delay. The exceptions to this rule are Connecticut

(90 days); Delaware (60 days); Florida (30 days); New Mexico (45 days); Ohio (45 days); Rhode Island (45 days); South Dakota (60 days); Vermont (45 days); Washington (45 days); and Wisconsin (45 days).

Some states require disclosure to additional entities regardless of the number of affected individuals: Maine (the appropriate state regulators in the Department of Professional and Financial Regulations or, if the entity is not regulated, the Attorney General); Montana (Attorney General's Office); New Hampshire (regulator with primary regulatory authority or the Attorney General's Office); New Jersey (Division of State Police in the Department of Law and Public Safety prior to disclosure to consumer); Oregon (Attorney General); South Dakota (all nationwide consumer reporting agencies); Vermont (Attorney General or Department of Financial Regulation within 14 days); and Virginia (Attorney General).

Other states require these additional disclosures if the number of individuals affected exceeds a certain threshold. States typically require all nationwide credit reporting agencies to be notified when there is a significant breach. Some states require additional agencies to be notified if a certain number of individuals are affected.

B. GEORGIA'S NOTIFICATION STATUTE, O.C.G.A. § 10-1-910 – 912

Georgia's notification statute, O.C.G.A. § 10-1-910 – 912, requires business that incur a data breach involving PII to notify affected Georgia residents as soon as possible through mail, telephone, or electronic means. If the breach affects more than 100,000 people or the cost of notification exceeds $50,000, other means of notification can be used (e.g., public service announcements). Additionally, a breach affecting more than 10,000 people must be reported to all credit reporting agencies.

C. FEDERAL NOTIFICATION LAWS

In 2014, Congress passed an updated version of the Federal Information Security Modernization Act (FISMA). FISMA establishes oversight and accountability for federal agencies in the area of data security and data breach reporting. As part of that oversight, the Office of Management and Budget created a uniform breach notification policy and guidelines for all federal agencies (the Breach Policy).

Under the Breach Policy, agencies are to include certain terms in every contract that will enable the agency to address a data breach involving a contractor. These terms include a requirement that contractors "cooperate with and exchange information with agency officials ... in order to effectively report and manage a suspected or confirmed breach" and that contractors must "report a suspected or confirmed breach . . . as soon as possible and without unreasonable delay."

D. THE GENERAL DATA PROTECTION REGULATION

The European Union's General Data Protection Regulation (Regulation (EU) 2016/679) took effect on May 25, 2018. Although the GDPR is a regulation applicable in the EU, its reach extends beyond the EU. The GDPR applies to businesses established in the EU and those that reach-out to individuals in the EU for business purposes. The intent is to protect people in the EU wherever their data may be located.

With limited exceptions, the GDPR applies to any person who processes personal data about an individual in the EU. Processing means collecting, storing, using, disclosing or otherwise performing operations on personal data.

V. DATA BREACH LAWSUITS

A. GENERAL

Plaintiffs allegedly affected by data breaches have pursued various legal theories in court. Generally brought as class actions, persons seeking redress have relied on common law, federal and state privacy rights, state consumer protection laws and contractual rights to try to establish a viable cause of action.

B. ARTICLE III STANDING

Persons affected by data breaches who sue in federal court due to exposure of their PII have to meet the standing requirement of Article III of the United States Constitution. To prove Article III standing a plaintiff must show: (1) she suffered an injury-in-fact; (2) her injuries were "fairly traceable" to defendant's actions; and (3) that a favorable judgment will redress her injuries. *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012). Plaintiff's "injury-in-fact" must be both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Id*. at 1323. Article III requires a threatened injury must be "certainly impending" to constitute an "injury-in-fact" when an actual injury has not yet occurred. *Clapper v. Amnesty International, USA*, 133 S. Ct. 1138, 1147 (2013).

In *Clapper*, plaintiffs were attorneys and organizations concerned about becoming subject to government surveillance pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) because there was "an objectively reasonable likelihood that their communications [would] be acquired [under FISA] at some point in the future." *Id*. at 1142-46. Defendants argued that a plaintiff alleging increased risk of future harm must establish the feared harm as "certainly impending" to

possess standing. The United States Supreme Court agreed, holding that the potential harm was not certain enough, the "threatened injury must be certainly impending to constitute injury in fact." *Id*. at 1147.

After *Clapper*, defendants in data breach cases often had claims dismissed based on the argument that plaintiffs had not alleged a sufficient injury-in-fact to meet Article III standing. In July 2015, however, the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 697 (7th Cir. 2015) held plaintiffs' fear of future harm from the breach was sufficient to establish standing to pursue claims.

Then, in May 2016, the United States Supreme Court, in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), held that to establish Article III standing, a plaintiff must show that she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Id*. at 1548.

Despite these decisions, there is a substantial split in the Circuits on whether potential future harm from a data breach is sufficient to provide Article III standing.

C. DAMAGES THEORIES

Damages theories include that a plaintiff, having had her PII compromised in a data breach, faces a heightened risk of future harm, e.g., the potential for criminals to use her data to commit identify theft. Other damages theories include negligence in protecting plaintiffs' sensitive information; breach of express and/or implied contract; breach of fiduciary duty; financial loss incurred in paying fees to close accounts and/or obtain new cards; financial loss incurred in paying for monitoring services; financial loss incurred from criminal use of a credit/debit card; breach of state consumer protection laws; and violation of the Fair Credit Reporting Act ("FCRA").

VI. CIRCUIT COURT SPLIT ON DATA BREACH LAWSUIT STANDING

A. THIRD, SIXTH, SEVENTH, NINTH, ELEVENTH AND D.C. CIRCUITS

THIRD CIRCUIT

On January 20, 2017, the Third Circuit in *Horizon Healthcare Services Data Breach Litigation*, 846 F.3d 625 (3d Cir. 2017), vacated a district court's dismissal of a data breach class action filed against Horizon Healthcare after a 2013 theft of two computer laptops containing unencrypted personal information of Horizon Healthcare plan members. The Third Circuit held that the plan members had standing to sue for alleged violations of the FCRA based on Horizon's alleged failure to adequately secure personal information against theft. The Third Circuit stated: "Even without evidence that the Plaintiffs' information was in fact used improperly, the alleged disclosure of their personal information created a *de facto* injury." *Id*. at 629.

On a November 2013 weekend, two laptop computers containing the unencrypted information of more than 839,000 Horizon plan members were stolen from Horizon's headquarters. The laptops were cable-locked to workstations and password protected, but the data stored on them was not encrypted. Upon discovery of the theft, Horizon immediately contacted the police and began an investigation. One month later, Horizon notified the impacted members and gave them one year of free credit monitoring.

On June 27, 2014, plaintiffs filed a class action complaint alleging violations of the FCRA and various state laws. In March 2015, the district court dismissed the complaint for lack of standing.

The district court held the plaintiffs had not alleged a sufficient injury-in-fact because they failed to allege economic loss caused by the data breach. The district court rejected the plaintiffs' argument that the alleged violation of the FCRA alone conferred standing.

On appeal, the Third Circuit reversed and held that a violation of the privacy protection right created by the FCRA was a sufficiently concrete injury. The Third Circuit noted the U. S. Supreme Court has "repeatedly affirmed the ability of Congress to 'cast the standing net broadly' and to grant individuals the ability to sue to enforce their statutory rights." *Id*. at 635. The Third Circuit held: "With passage of the FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself - whether or not the disclosure of that information increased the risk of identity theft or some other future harm." *Id*. at 639. Because the FCRA creates a private "remedy for the unauthorized transfer of personal information, a violation of the FCRA gives rise to an injury sufficient for Article III standing purposes." *Id*. at 629.

SIXTH CIRCUIT

The Sixth Circuit in *Galaria v. Nationwide Mut. Ins. Co*., 663 Fed. Appx. 384 (6th Cir. 2016) held allegations of increased risk of future harm are sufficient to satisfy the injury-in-fact element of Article III standing. In *Galaria*, the Sixth Circuit reversed the Southern District of Ohio's ruling that the plaintiffs' initial putative class action complaint failed to allege injury-in-fact because no actual harm was alleged, rather only the increase of future harm. The district court held mitigation costs incurred to prevent alleged future harm were insufficient to satisfy the injury-in-fact element of standing

because plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014), quoting *Clapper, Supra*, at 1146.

The Sixth Circuit, however, disagreed with the district court and held plaintiffs' allegations of an increased risk of harm and mitigation costs incurred in an effort to prevent such future harm were sufficient to demonstrate standing.

SEVENTH CIRCUIT

The Seventh Circuit considered similar arguments in *Pisciotta v. Old Nat. Bancorp,* 499 F.3d 629 (7th Cir. 2007). Plaintiffs in that case sued their bank after a data breach resulted in the disclosure of their names, social security numbers, drivers' license numbers, birth dates, mothers' maiden names, credit card, and other financial account numbers. The Seventh Circuit held "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 the defendant's actions," *Id*. at 634, and thus plaintiffs had standing to sue due to their allegations that defendant's breach created an increased risk of future harm.

The Seventh Circuit, however, affirmed the district court's dismissal, holding that although the plaintiffs alleged injury in the form of increased risk of future harm, that increased risk could not constitute the damages necessary to maintain their claims.

In July 2015, the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015) held plaintiffs' fear of future harm from a data breach was sufficient to establish Article III standing to proceed with a nationwide class action arising from the breach of payment card data at Neiman Marcus stores.

In January 2014, Neiman Marcus publicly disclosed that between July 16, 2013 and October 30, 2013 malware installed in its computers had attempted to collect account information from 350,000 cards - and 9,200 cards (from the 350,000) were fraudulently used. Neiman Marcus reimbursed fraudulent charges and offered all 2013 customers one year of free credit card monitoring and identity theft protection.

In July 2014, four named plaintiffs, who allegedly made card purchases from Neiman Marcus in 2013, sued Neiman Marcus under the Class Action Fairness Act alleging negligence, breach of implied contract, violations of state unfair and/or deceptive practices statutes, violations of state data breach notification laws and other state remedies. Plaintiffs argued they had standing based on alleged present and future injury, including: (1) lost time and money resolving the fraudulent charges; (2) lost time and money protecting themselves against future identity theft; and (3) an increased risk of future fraudulent charges and greater susceptibility to identity theft. The four named plaintiffs proposing to represent a nationwide class.

The district court dismissed on the grounds that the named plaintiffs and class lacked Article III standing. Plaintiffs appealed to the Seventh Circuit – which reversed. The Seventh Circuit acknowledged that to prove standing a plaintiff must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision." *Id*. at 691 – 692.

The Seventh Circuit, however, held: "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such injury will occur." *Id*. at 693. It further held: "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" are injuries sufficient to satisfy the injury requirement for Article III standing. *Id*. at 696.

On April 11, 2018, the Seventh Circuit in ***Dieffenbach v. Barnes & Noble, Inc.***, 887 F.3d 826 (7th Cir. 2018) reinstated a data breach class action against Barnes & Noble, after an Illinois federal district court dismissed it for lack of standing. In reversing, the Seventh Circuit held that two victims of a 2012 Barnes & Noble data breach had standing to sue and could pursue state law claims in California and Illinois.

The claims arose from a September 2012 data breach in which "skimmers" breached PIN pads that Barnes & Noble used to verify payment information and obtained customers' names, card numbers and expiration dates and PINs. Some customers lost the use of their funds while waiting for banks to reverse unauthorized charges to their accounts; some customers spent money on credit-monitoring services; and some customers spent time getting new account numbers and notifying businesses of the changes. Two consumers filed a putative class action lawsuit against Barnes & Noble, which the district court dismissed for lack of standing.

The Seventh Circuit reversed, holding the plaintiffs had standing because the data theft may have caused them to spend money and incur opportunity-costs in "one's own time needed to setting things straight." *Id*. at 828. The Seventh Circuit noted that one plaintiff filed suit under California consumer protection statutes alleging: (1) her

bank took three days to restore funds someone else used fraudulently; (2) she had to spend time sorting-out her affairs with the police and a bank; (3) she could not make purchases with her compromised account for three days; and (4) she did not receive the benefit of her bargain with Barnes & Noble. The Seventh Circuit held the first three claims were sufficiently pled to confer standing to sue. *Id*. at 829.

The second plaintiff brought claims under Illinois consumer protection laws alleging: (1) her bank contacted her about a potentially fraudulent charge on her credit card statement and deactivated her account; and (2) the security breach prompted her to renew a credit monitoring service subject to a monthly charge. The Seventh Circuit held these alleged harms were sufficient actual damages to proceed with claims under the state statutes. *Id*. at 829 – 830.

Although the Seventh Circuit allowed the case to proceed, it noted that its ruling only addressed standing to sue: "All we hold today is that the complaint cannot be dismissed on the ground that the plaintiffs do not adequately allege compensation damages." Additionally, the Seventh Circuit noted that Barnes & Noble was also a victim of the data breach that suffered economic damages and stated: "Plaintiffs may face a difficult task showing an entitlement to collect damages from a fellow victim of the data thieves." *Id*. at 830.

NINTH CIRCUIT

The Ninth Circuit in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), also addressed plaintiffs' alleged risk of future harm damages in a data breach case. In *Krottner*, a putative class of current and former Starbucks employees sued Starbucks after a company laptop containing their names, addresses, and social

security numbers was stolen. Plaintiffs alleged that Starbuck's failure to reasonably protect their highly sensitive information was negligent and a breach of implied contract. The district court dismissed the case because plaintiffs failed to show any identity theft from the breach and failed to show they suffered economic harm. The Ninth Circuit reversed, holding that because of the highly sensitive nature of the improperly accessed information, plaintiffs faced a "credible threat of real and immediate harm" and therefore satisfied the injury-in-fact requirement for Article III standing. *Id*. at 1143.

On March 8, 2018, the Ninth Circuit, in *In re Zappos.Com, Inc.* In, 884 F.3d 893 (9th Cir. 2018), reversed a data breach decision from the USDC for the District of Nevada. The district court held that one sub-class of plaintiffs did not sufficiently allege injury-in-fact to establish Article III standing. The district court's opinion focused on consumers who did not allege that any fraudulent charges had been made using their identities, despite hackers accessing their names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information in a 2012 data breach.

The Ninth Circuit, however, held the theft of a laptop containing consumers' personally identifying information raised a credible threat of real and immediate harm. In *Clapper,* the U.S. Supreme Court held the "objectively reasonable likelihood" that plaintiffs' communications would be swept up in FISA surveillance did not rise to level of a "certainly impending injury" necessary to establish Article III standing. *Supra*, 133 S.Ct. at 1150. The Ninth Circuit noted the series of inferences alleged by the *Clapper* plaintiffs, where none of their communications had yet been intercepted. In

Krottner, however, the thief had acquired all of the information necessary to steal the plaintiffs' identities once she accessed the stolen laptop. Similarly, in *In re Zappos,* the Ninth Circuit reasoned the plaintiffs had alleged that hackers had accessed enough data to enable the hackers to steal their identities.

The Ninth Circuit, however, left open the possibility that plaintiffs might not be able to present sufficient evidence to support standing at summary judgment.

ELEVENTH CIRCUIT

The Eleventh Circuit in *Resnick v. AvMed*, 693 F.3d 1317 (11th Cir. 2012), reversed a lower court's data breach decision and held a class of plaintiffs suing AvMed for allowing its personal information to be stolen had shown both sufficient injury and causation to survive AvMed's motion to dismiss the claims.

The claims arose from a December 2009 incident in which two unencrypted laptops containing the personal information of approximately 1.2 million current and former subscribers to AvMed were stolen from AvMed's corporate offices in Florida. The computers had customers' protected health information, Social Security numbers, names, addresses and phone numbers. A criminal used that information to steal individuals' identities. Two of the effected individuals filed a complaint in the Southern District of Florida on behalf of the class alleging that AvMed was: (1) negligent in protecting plaintiffs' sensitive information; (2) negligent per se for failing to protect plaintiffs' medical information; (3) in breach of contract for failing to protect plaintiffs' information; and (4) in breach of fiduciary duties owed the plaintiffs.

AvMed filed a motion to dismiss for failure to state a claim. The district court granted the motion and dismissed the claims based on a lack of evidence of injury to

plaintiffs and causation between the security breach and the plaintiffs having their identities stolen. Plaintiffs appealed to the Eleventh Circuit.

On appeal, the Eleventh Circuit first addressed whether a party claiming identity theft resulting from a data breach had suffered an injury-in-fact and concluded the monetary damages the class plaintiffs alleged as a result of the identity theft constituted injury-in-fact. The Eleventh Circuit then addressed whether AvMed's actions caused the plaintiffs' injury-in-fact and concluded that such injury was traceable to AvMed's failure to properly secure the information. Having concluded that the plaintiffs were injured and such injury was caused by AvMed, the Eleventh Circuit held plaintiffs had standing to bring the case.

Next, the Eleventh Circuit held the plaintiffs properly stated claims for negligence, breach of contract and breach of fiduciary duties -- but did not state a claim for negligence per se. The Eleventh Circuit reasoned that if plaintiffs showed a causal relationship between AvMed's failure to secure their personal information and the alleged theft of plaintiffs' identities, then they could survive AvMed's motion to dismiss. The Eleventh Circuit found the evidence showed a link between the information compromised in the data breach and the data used to steal the plaintiffs' identities. Thus, the plaintiffs proved causation. With regard to the negligence per se claim, the Eleventh Circuit upheld the dismissal of that claim because it held that AvMed was not subject to Florida's Negligence Per Se Statute.

Resnick was decided before the U.S. Supreme Court's decision in *Clapper.*

D.C. CIRCUIT

On August 1, 2017, the D.C. Circuit in *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) held that fear of future harm is sufficient for consumer data breach claimants to establish standing.

In June 2014, CareFirst, a health insurer, suffered a data breach. Several CareFirst customers filed a data breach class action asserting 11 state law causes of action including breach of contract, negligence, and violation of state consumer protection statutes. Defendant filed a motion to dismiss arguing plaintiffs failed to show standing because their alleged injuries were not sufficiently concrete. The district court agreed and held plaintiffs' allegations of risk of future identify theft was too speculative and they failed to show how hackers could steal their identities based on the information that had been accessed. Plaintiffs appealed to the D.C. Circuit.

The D.C. Circuit reversed the district court, holding the plaintiffs "have cleared the low bar to establish standing at the pleading stage." *Id*. at 622. In reaching that decision, the D.C. Circuit said "nobody doubts that identify theft, should it befall one of these plaintiffs, would be constitute a concrete and particularize injury." *Id*. at 627. The D.C. Circuit said the remaining question was "whether the complaint plausibly alleges that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence." *Id*. at 627.

The D.C. Circuit said the district court's conclusion that plaintiffs had not met these requirements rested on an "incorrect premise" that the complaint did not allege the theft of social security or credit card numbers that would facilitate identity theft." *Id*. at 627. The D.C. Circuit determined the complaint alleged theft of

categories of information that included social security and credit card information, and the combination of information the plaintiffs alleged was stolen "make up, at the very least, a plausible allegation that plaintiffs face a substantial risk of identify fraud, even if their social security numbers were never exposed." *Id*. at 627 - 628.

The D.C. Circuit said "it is much less speculative – at the very least, it is plausible – to infer that [the hacker] has both the intent and ability to use that data for ill." *Id*. at 628. It cited the Seventh Circuit's statement in *Remijas*: "Why else would hackers break into a ... database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those customers' identity." *Id*. at 628 - 629.

B. FIRST, SECOND, FOURTH AND EIGHTH CIRCUITS

FIRST CIRCUIT

The First Circuit, in *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011), held that under Maine law plaintiffs could recover mitigation costs arising from a data breach.

The claims arose from a 2007 breach of Hannaford's electronic payment processing system, which resulted in the theft of 4.2 million credit and debit card numbers. In March 2008, Hannaford announced the breach and noted it received reports of 1,800 cases of fraud resulting from the breach. After that announcement, some financial institutions canceled customers' credit and debit cards and issued new cards. Other financial institutions monitored customer accounts for unusual activity. Some customers paid fees to cancel their cards and get new cards, and some bought identity theft insurance and credit monitoring services due to the breach.

Plaintiffs alleged: (1) breach of implied contract; (2) breach of implied warranty; (3) breach of duty of a confidential relationship; (4) failure to advise customers of the theft of their data; (5) strict liability; (6) negligence; and (7) violation of Maine's Unfair Trade Practices Act (UTPA).

Hannaford filed a motion to dismiss and the district court granted the motion as to 20 of the 21 plaintiffs. The only plaintiff who survived the motion to dismiss was the only one who alleged she had unreimbursed fraudulent charges to her account. As for the other plaintiffs, the district court held they failed to state claims under Maine law for breach of fiduciary duty, breach of implied warranty, strict liability and failure to notify customers of the data breach. The district court also found the plaintiffs adequately alleged breach of implied contract, negligence and violation of UTPA, but that their alleged injuries were "too remote, not reasonably foreseeable and/or speculative" to be recognized under Maine law. *In re Hannaford Bros. Co Customer Data Sec. Breach Litig*., 613 F. Supp. 2d 108, 134 (D. Me. 2009). The district court also held there was no way to value or compensate the time and effort customers spent to reverse or protect against losses, and that there was no allegation to justify the claim for identity theft insurance since no personally identifying information was alleged to have been stolen. *Id*. at 134 – 135.

After ruling on the motion to dismiss, the district court certified the following question to the Supreme Judicial Court of Maine: "In the absence of physical harm or economic loss or identity theft, do time and effort alone, spent in a reasonable effort to avoid or remediate reasonably foreseeable harm, constitute a cognizable injury for which damages may be recovered under Maine law of negligence and/or implied

contract?" *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492 (Supreme Judicial Court of Maine 2010).

The Supreme Judicial Court of Maine answered the question in the negative, holding that time and effort alone do not constitute a cognizable claim under Maine law.

Plaintiffs then appealed to the First Circuit, which partially reversed the district court's decision. The First Circuit held that plaintiffs' claims for negligence and implied contract survived the motion to dismiss because their reasonably foreseeable mitigation costs were cognizable claims for damages under Maine law.

The First Circuit noted that Maine law encourages plaintiffs to take reasonable steps to minimize losses caused by a defendant's negligence. *Id*. at 162. Considering the Restatement (Second) of Torts sec. 919, the First Circuit said: "It was foreseeable, on these facts that a customer, knowing that her credit or debit card had been compromised and that thousands of fraudulent charges had resulted from the same security breach, would replace the card to mitigate against misuse of the card data." *Id*. at 164. Thus, the First Circuit held: "Plaintiffs' claims for identity theft and replacement card fees involve actual financial losses from credit and debit card misuse. Under Maine contract law, these financial losses are recoverable as mitigation damages as long as they are reasonable." *Id*. at 167.

With regard to the implied contract claim, the First Circuit held a jury could reasonably find an implied contract between Hannaford and its customers pursuant to which Hannaford would take reasonable measures to protect the information.

The First Circuit, however, rejected plaintiffs' other claims. It held the fiduciary/confidential relationship claim failed because Hannaford did not owe a fiduciary

duty to its customers. It held: (1) plaintiffs did not prove the trust and confidence contemplated by Maine confidential relationship cases; (2) plaintiffs did not plead facts demonstrating disparate bargaining power between them and Hannaford; and (3) plaintiffs failed to allege facts demonstrating that Hannaford abused a position of trust.

The First Circuit also rejected plaintiff's UTPA claim, stating: "It seems unlikely to us that Maine would permit plaintiffs, in cases also pleading that the same acts constitute negligence and breach of implied contract, to use the right of private action provision of the UTPA to recover types of damages which Maine has decided are not reasonably foreseeable or barred for policy reasons when asserted under implied contract, negligence or other theories." *Id*. at 161.

On February 28, 2012, the First Circuit in *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012), affirmed a district court's ruling that a data breach plaintiff lacked Article III standing to sue a financial services company for breach of common law rights and violation of a state consumer protection law by failing to provide adequate data security measures and prevent the potential disclosure of her private.

The issue in that case was whether plaintiff had Article III standing to sue a defendant because of its inadequate data security failed to prevent the potential disclosure of her private personal information, when the plaintiff did not have a contract with the defendant and did not allege her private data was accessed.

Defendant sold investment products and services, including an electronic platform that gave subscribing financial organizations an interface for managing brokerage accounts online. A subscribing financial organization using that electronic platform could make its clients' private information, including social security numbers

and taxpayer identification numbers, accessible to authorized employees within the organization.

The plaintiff had a brokerage account at National Planning Corporation (NPC), a financial organization that used defendant's electronic platform. Defendant and NPC were parties to a contract. Defendant and the plaintiff, however, did not have a contract. After NPC made its customers' information accessible on defendant's electronic platform, defendant sent plaintiff a disclosure statement informing her about the provisions of its contract with NPC.

Plaintiff sued defendant alleging it failed to protect her private information as required by contract and statutory consumer protection laws. Defendant moved to dismiss on the grounds that plaintiff lacked Article III standing. The USDC for the District of Massachusetts held the plaintiff lacked constitutional and statutory standing and dismissed her claims.

The First Circuit affirmed the district court's decision and dismissed plaintiff's common law contract and statutory consumer protection claims and held she lacked Article III standing to sue.

SECOND CIRCUIT

The Second Circuit, in *Whalen v. Michaels Stores*, 689 Fed. Appx. 89 (2nd Cir. 2017), affirmed the district court's dismissal of a plaintiff's data breach complaint, holding she did not allege any injury that met the standing requirements of Article III.

On January 25, 2014, Michaels Stores notified its customers in press release of "possible fraudulent activity on some U.S. payment cards." On April 17, 2014, Michaels confirmed a data breach in a press release, but reported there was no evidence that the

hackers had obtained any other customer information, such as names, addresses, or PIN numbers. Michaels estimated that about 2.6 million payment cards may have been affected between May 8, 2013 and January 27, 2014, and offered free identity protection and credit monitoring services for twelve months to affected customers.

Mary Jane Whalen made purchases with her credit card at a Michaels store on December 21, 2013. On January 14 and 15, 2014, her credit card information was used unsuccessfully in two attempted fraudulent transactions in Ecuador. On January 15, 2014, she cancelled her credit card and no other fraudulent transactions were either incurred or attempted on her card.

On December 2, 2014, Whalen filed a putative class action against Michaels, alleging: (1) her credit card information was stolen and used in two attempted fraudulent transactions; (2) she faced a risk of future identity theft; and (3) she had lost time and money resolving the attempted the fraudulent charges and monitoring her credit. She claimed damages based on breach of implied contract and violation of New York General Business Law § 349. The district court dismissed the complaint, holding Whalen lacked standing because she "neither alleged that she incurred any actual charges on her credit card, nor, with any specificity, that she had spent time and money monitoring her credit." *Id*. at 90.

The Second Circuit affirmed the district court's dismissal, holding Whalen "alleged no injury that would satisfy the constitutional standing requirements of Article III." *Id*. at 91. It held: "Whalen does not allege a particularized and concrete injury suffered from the attempted fraudulent purchases… she never was either asked to pay, nor did pay, any fraudulent charge. And she does not allege how she can plausibly face

a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen." The Second Circuit also held: "Whalen pleaded no specifics about any time or effort that she herself ha[d] spent monitoring her credit," instead relying on the general allegation that the putative class had suffered damages based on "the opportunity cost and value of time" they had been forced to expend to monitor their financial accounts. *Id*. at 90 – 91.

On November 21, 2017, the Second Circuit in *Santana v. Take-Two Interactive Software, Inc*., 717 Fed. Appx. 12 (2nd Cir. 2017), affirmed the dismissal of a class action lawsuit brought in the Southern District of New York under the Illinois Biometric Information Privacy Act (BIPA) for lack of standing.

Take-Two Interactive Software Inc. published a video game which includes a feature allowing players, like the plaintiffs, to scan their faces for use in the game. Plaintiffs alleged that, using this feature, players scanned their faces and provided it as "biometric information" to Take-Two. They also alleged that Take-Two did not follow certain notice, consent, storage, security and dissemination provisions of BIPA regarding the face scan. Specifically, they alleged: (1) Take-Two did not provide notice about its retention schedule or guidelines for destroying the biometric data; (2) Take-Two failed to obtain proper consent by informing the plaintiffs in writing that biometric data would be collected and the purposes and length of that collection; (3) Take-Two failed to obtain proper consent by obtaining a written release; (4) Take-Two disclosed and disseminated data without obtaining adequate consent; and (5) Take-Two failed to transmit the biometric data securely.

Plaintiffs asserted other tort theories of liability stemming from these violations, including claims that they were apprehensive about engaging in future biometric-facilitated transactions.

Take-Two moved to dismiss the complaint based on a lack of Article III and state statutory standing. The district court dismissed the claims with prejudice, relying on *Spokeo, Supra,* and *Strubel v. Comenity Bank*, 842 F.3d 181 (2nd Cir. 2016) to conclude the plaintiffs did not adequately allege a "material risk of harm to" the "concrete interests" protected by the statute. *Vigil v. Take-Two Interactive Software, Inc*., 235 F. Supp. 3d 499, 511 (S.D. NY 2017). The district court also rejected the related tort claims stemming from the statutory violations as attempts to "manufacture an injury-in-fact." *Id*. at 515. Plaintiffs appealed to the Second Circuit.

On appeal, the Second Circuit affirmed the district court's ruling that the plaintiffs lacked Article II standing to bring claims under BIPA because none of the alleged procedural violations of BIPA raised a material risk of harm to the plaintiffs' interest in preventing unauthorized use of their private information. The Second Circuit, however, held the district court erred in dismissing the complaint with prejudice for failure to state a cause of action under BIPA, because a finding that the players were not "aggrieved parties" as used in BIPA was a judgment on the merits that could not be addressed absent subject matter jurisdiction.

FOURTH CIRCUIT

On June 12, 2018, the Fourth Circuit in *Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018), held plaintiffs alleged sufficient injury to meet the Article III standing requirement by virtue of hackers' theft and misuse of

plaintiffs' personally identifiable information, notwithstanding the absence of any allegation that the misuse had resulted in pecuniary loss to the plaintiffs.

The plaintiffs were three optometrist members of the National Board of Examiners in Optometry, Inc. (NBEO) who on different dates submitted their personal information to the NBEO. In July 2016, optometrists across the country noticed that Chase Amazon Visa credit cards had been fraudulently opened in their names. The creation of those fraudulent accounts, which required the use of an applicant's social security number and date of birth, convinced several of persons that data containing their personal information had been stolen. They determined that the NBEO was the only common source to which they had given their personal information.

The NBEO soon became aware of the concerns and in August 2016 issued a statement that its data systems had not been compromised. Three weeks later the NBEO revised its announcement and stated it was still investigating, but it never said its data systems were breached.

The plaintiffs sued the NBEO alleging negligence, breach of contract, breach of implied contract and unjust enrichment. One plaintiff alleged damages in the form of time and money spent implementing credit freezes with the three credit agencies. The second plaintiff alleged damages from her time and effort submitting reports to the FTC, IRS and the FBI. The third plaintiff alleged her credit score was decreased shortly after a false credit card application and that Chase Amazon demanded certified letters and a police report to remedy the dispute over her credit score.

The NBEO moved to dismiss based on lack of Article III standing. The district court granted the motion, citing *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), a case

in which there was no evidence that information on a stolen laptop had been accessed or misused and, therefore, there was no injury-in-fact. Plaintiffs appealed to the Fourth Circuit.

On appeal, the Fourth Circuit reversed and held that under the facts alleged in the complaints the plaintiffs had Article III standing. The Fourth Circuit acknowledged that "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Id*. at 621. It, however, held that although the plaintiffs did not show actual economic loss, they showed that credit cards had been opened in their names, expenses incurred to seek credit monitoring and in some cases credit scores were adversely affected. *Id*. at 622. Thus, the Fourth Circuit held the plaintiffs met the injury-in-fact element.

With regard the element of traceability of the harm to the defendant's act, the Fourth Circuit noted that specific pleadings had identified plausible evidence, such as allegations of credit cards opened in the name of several plaintiff's maiden names that have been given to the NBEO many years earlier, that the NBEO was a plausible source of the plaintiffs' personal information.

Having found that the standing elements of injury-in-fact and traceability were both sufficiently alleged in the complaints, the Fourth Circuit held that the district court erred in dismissing the complaints for lack of standing to sue.

EIGHTH CIRCUIT

In August 2017, the Eighth Circuit, in *In re SuperValu, Inc. Customer Data Security Breach Litigation*, 870 F.3d 763 (8th Cir. 2017), dismissed most of a class action case on appeal from the USDC for the District of Minnesota for lack of standing.

Plaintiffs' claims arose from two 2014 breaches in which customers' credit card data was believed to be stolen from SuperValu. Although plaintiffs alleged they believed illicit websites were selling their credit card information, the Eighth Circuit held the allegations were "speculative" and "fail[ed] to allege any injury 'to the plaintiff[s]'" (rather than injury to plaintiffs' credit card companies, which spent money to mitigate the potential fraud). Because the breaches involved only credit card information and not sufficient information to open new credit accounts, the Eighth Circuit held plaintiffs' allegations of "future harm" were too speculative. *Id*. at 770 – 771. The Eighth Circuit allowed one named plaintiff's case to proceed because he alleged his credit card information was used and he had to cancel it.

The Eighth Circuit, however, in another case, *Kuhns v. Scottrade, Inc.,* 868 F.3d 711 (8th Cir. 2017), dismissed a class action, but only after finding the plaintiffs sufficiently alleged standing by asserting a breach of contract claim.

A 2013 data breach of Scottrade allegedly resulted in hackers acquiring personal identifying information of more than 4.6 million Scottrade customers. The hackers allegedly exploited the information in multiple ways, including by manipulating stock prices.

The plaintiff "alleged that he bargained for and expected protection of his PPI, that Scottrade breached the contract when it failed to provide promised reasonable safeguards, and that [the plaintiff] suffered actual injury, the diminished value of his bargain." *Id*. at 716.

The Eighth Circuit relied on its 2016 holding in *Carlsen v. GameStop, Inc.*, 833 F.3d 903 (8th Cir. 2016), where it held that when a company, as part of a contract,

promises to protect personal information and fails to do so, parties to the contract have suffered an injury sufficient to have standing. Eighth Circuit in *Kuhns* held: "Whatever the merits of Kuhns's contract claim, and his related claims for breach of implied contract and unjust enrichment, he has Article III standing to assert them." *Id*. at 716. The Eighth Circuit, however, dismissed the case because the complaint "fail[ed] to allege a specific breach of the express contract." *Id*. at 717.

VII. GEORGIA COURT OF APPEALS DECISION ON STANDING IN DATA BREACH LAWSUITS

Collins v. Athens Orthopedic Clinic, 815 S.E. 2d 639, 2018 Ga. App. LEXIS 440 (June 27, 2018), is the first the Georgia Court of Appeals case to address the issue of standing in a data breach case.

This case arose from a data breach at Athens Orthopedic Clinic. The hacker stole PII of more than 200,000 current and former patients of the clinic. Plaintiffs filed a putative class action alleging violation of the Georgia Uniform Deceptive Trade Practices Act, breach of implied contract, unjust enrichment and negligence. They alleged damages related to costs incurred and future costs to be incurred for the purchase of credit monitoring and identity theft protection, or the placing of credit freezes on their accounts. Defendant filed a motion to dismiss based on lack of Article III standing. The trial court granted the motion and plaintiffs appealed.

The Georgia Court of Appeals affirmed the trial court's decision and held the plaintiffs' damages claims, which specified only the cost of identity theft protection, credit monitoring, and credit freezes to be maintained "over the course of a lifetime,"" was speculative and insufficient to state a cognizable claim under Georgia law.

VIII. CONCLUSION

The digitalization of life will continue to expand in ways we can only imagine – and in unimaginable ways. Computerized systems, smart cars, smart home security, smart homes, smart home appliances, smart surveillance cameras, smart televisions, smart phones, Smart airplanes, smart locks, Alexa, Siri, Google Assistant, Cortana, A.I., Watson, Amazon Echo, Google Home, the cloud, the internet of things, biometric authentication, fingerprint recognition, voice recognition, retina recognition systems, facial recognition systems, Iris recognition, palm vein recognition systems, J.A.R.V.I.S.?, Skynet?. With the possible exception of J.A.R.V.I.S. and Skynet, these are just a few of the technologies that can impact private information. The gateways to personal information are numerous and rapidly expanding. All such gateways are potential data breach concerns and as the gateways expand, so too do the opportunities for criminals to steal private information. The law has to keep pace with this continuing evolution, and lawyers must be vigilant in addressing the law to meet these changes.