SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Key Cyber Risk Insurance Coverage, Data Breach, and Standing Decisions 2017

Vincent J. Vitkowsky

New York Connecticut New Jersey

SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Key Cyber Risk Insurance Coverage, Data Breach, and Standing Decisions 2017

Coverage Decisions

Overview

The principal cyber risks in 2017 were data breaches, ransomware, cyber extortion, lost data, network disruption, business interruption, resulting property damage, and liability from websites and social media. In addition, losses from fraudulent funds transfers induced by social engineering have come to be thought of as a cyber risk.

Over the years, some key decisions have involved claims for network disruption, business interruption and lost data under property policies. The results were split, with some finding coverage. That resulted in the introduction of cyber exclusions in many policies. But there is a recent tendency by some property insurers to allow coverage. Some have actively marketed the fact that they provide coverage. Others go farther. For example, at least one insurer has introduced a Cyber Optimal Recovery Endorsement to its all-risk policy. When the insured also has cyber insurance, the endorsement gives the insured the option of choosing whether the all-risk policy is primary, contributing, or excess -- whatever will maximize recovery.

There have also been cases seeking coverage for data breaches under CGL Coverage B, personal and advertising liability. Two decisions found coverage, and three – including one in 2017 – have found no coverage.

There is still only one reported decision addressing coverage for a data breach under a policy specifically designed as a cyber insurance policy. That is ***P.F. Chang's China Bistro, Inc v. Federal Ins. Co.***, 2016 WL 3055111 (D. Ariz. May 31, 2016), which held there was no coverage for Payment Card Industry Fees and Assessments under the specific language of the Policy involved. The decision was based on multiple grounds, and the lead ground was that the contractual liability exclusion barred coverage. The decision is on appeal.

Finally, there has been much litigation seeking coverage for fraudulent funds transfers, often but not always induced by social engineering, under crime policies. With one notable exception, the 2017 cases found no coverage.

In 2017, there were nine noteworthy coverage decisions concerning cyber risks under various lines of business.

Media Liability Coverage under Cyber Policy

New York Appellate Division Applies Retroactive Date Exclusion and Unfair Practices Exclusion to Deny Coverage under a Comprehensive Cyber Policy

LifeLock, Inc. v. Certain Underwriters at Lloyd's, 146 A.D.3d 565, 2017 WL 161045 (N.Y. App. Div. Jan. 17, 2017). The First Department affirmed the dismissal of claims seeking media liability coverage under an Information Security, Privacy Liability, First Party Data Protection and Network Business Interruption Insurance Policy.

LifeLock is an identity theft protection company. It was sued in several class actions asserting that, through statements on its website, it had engaged in fraudulent and deceptive practices to induce customers to enter into contracts that did not provide the protections it promised.

The Retroactive Date Exclusion precluded coverage for "related or continuing acts ... where the first such act … was committed or occurred prior to the Retroactive Date." The statements first appeared on LifeLock's website in 2005 and remained after the Retroactive Date of January 8, 2008. Underwriters argued that there was pattern of false and misleading advertising beginning in 2005, so the Exclusion applied. The court agreed. In addition, Underwriters argued that the claims fell within the Exclusion for Unfair Trade Practices. Again, the court agreed.

Data Breach Coverage under Management and D&O Policy

Texas Federal District Court Dismisses a Claim for Coverage of Attorneys' Fees Incurred to Recover PCI Fees and Fines Withheld by a Card Processor

Spec's Family Partners Ltd. v. Hanover Ins. Co., 2017 WL 32780060 (S.D. Tex. Mar. 15, 2017). The court dismissed a retailer's claim for coverage of attorneys' fees incurred in an action to recover PCI fees and fines withheld by a card processor. The decision was based on the absence of coverage because of the contractual liability exclusion.

The case arose under a Private Company Management Liability Policy with a Directors, Officers and Corporate Liability Coverage Part issued by Hanover Insurance Company to Spec's, a chain of liquor stores in Texas. Spec's suffered two data breaches of its credit card payment system. Its transactions were processed pursuant to a Merchant Agreement with First Data Merchant Services, LLC.

Visa and MasterCard issued $9.5 million in case management fees and assessed fines (collectively, "fines"). First Data sent two letters to Spec's for claims arising from the

data breaches. To satisfy its demands, First Data withheld $4.2 million from daily payment card settlements for Spec's and used the money to establish a reserve account. Spec's sued First Data to seek recovery of the withheld amounts. It also sued Hanover, which had entered into a Defense Funding Agreement ("DFA"), arguing that Hanover should pay for its lawyers in the action against First Data.

The court granted Hanover's motion to dismiss on the pleadings, resolving the case by holding that there was no duty to defend of any kind, because coverage was precluded by the exclusion for liability under a contract.

The policy gave Hanover the right and duty to defend a "Claim," which was defined to include a written demand for monetary damages for a Wrongful Act. The court found that the fines were levied against the card processor, First Data, and did not represent a separate demand against Spec's, so were not a Claim under the policy. Rather, the Claim was made in the demand letters for indemnification under the Merchant Agreement.

In applying the contractual exclusion, the court reviewed the DFA to determine whether it modified the exclusion, and concluded it did not, because in the DFA, Hanover reserved its rights to challenge its duty of defense or to withdraw its defense. The court went on to reject the contention that the fines and the funding of a reserve account did not arise out of the contract with First Data, so were covered because the exclusion did not apply if the liability would have attached in the absence of the contract. The court declined "to find a speculative factual scenario or legal theory in which MasterCard or Visa make a claim directly against [the insured]." It found the only Claim was the one for indemnification in the demand letters.

The court also rejected the insured's argument that the hack constituted superseding criminal conduct, which was an independent, "but for" cause of the claim making the contractual exclusion inapplicable. The court held that the only reason for the liability of Spec's to First Data was the Merchant Agreement. The decision is on appeal.

Data Breach and Cyber-related Privacy Coverage under CGL Coverage B

Ninth Circuit Finds No Coverage under Coverage B for Installation of Spyware and Capturing of Private Information

American Economy Ins. Co. v. Hartford Fire Ins. Co., 695 Fed.Appx 194, 2017 WL 2323440 (9th Cir. May 26, 2017).The Ninth Circuit addressed whether a duty to defend existed where there were allegations that the insured installed spyware on rented laptops that allowed access to keystrokes and screenshots. The insured sought coverage for "bodily injury" and "personal and advertising injury" under CGL Coverage B.

There were two underlying cases, one by consumers and one by the State of Washington. Applying Montana law, the court held that coverage for the Washington

action was precluded because of the failure to allege publication, and in both cases by an exclusion for Recording and Distribution of Material in Violation of Law. The court held that the insurers were entitled to recoupment of defense costs which had been advanced, because the insured "implicitly accepted" their defenses under a reservation of rights.

Florida Federal District Court Finds No Duty to Defend under CGL Coverage B for a Data Breach Caused by Hackers

Innovak International, Inc. v. The Hanover Ins. Co., 2017 WL 5632718 (M.D. Fl. Nov. 17, 2017). Applying South Carolina law, the court found no coverage and hence no duty to defend a putative class action under Coverage B of a CGL policy on the grounds that third-party hackers, not the Insured, caused the data breach.

The Insured designs, develops, and sells accounting and payroll computer software systems to schools, school districts, and other entities. Hackers acquired personal private information ("PPI") stored on its software, database, and/or portals. The court noted that the underlying claimants "did not allege publication, that is, public dissemination of their PPI, but instead alleged appropriation of their information by third-party hackers." They asserted claims for negligence, breach of implied contract, gross negligence, unjust enrichment, and fraudulent suppression. The court found the "only plausible interpretation of Coverage B is that it requires the insured to be the publisher of the PPI." It rejected arguments that the insured "published software."

The policy also contained a separate Data Breach Form, but it did not cover third-party liability. In a footnote, the court "noted" that the form might have limited any coverage available under Coverage B, but it did not need to reach the issue given its finding there was no coverage.

Fraudulent Funds Transfers under Crime Policies

Decisions Finding No Coverage

Ninth Circuit Finds No Coverage under a Crime Policy for Social Engineering-induced Fraudulent Funds Transfer

Taylor & Lieberman v. Federal Ins. Co., 681 Fed.Appx 627, 2017 WL 929211 (9th Cir. Mar. 9, 2017). The Ninth Circuit held that an accounting and business management firm that fell victim to a social engineering fraud did not have coverage under any of the insuring agreements of a Crime Policy.

The insured received two emails from a client's hijacked email account, directing funds transfers to accounts in Malaysia and Singapore. It complied. The insured then received a third email purportedly from the client, but from another email address, directing a third transfer. The insured called the client and learned that all three emails were fraudulent.

The Forgery grant applied to "forgery or alteration of a financial instrument." The insured argued quaintly that under the "Last Antecedent Rule," the word" alteration" only applied to "financial instruments", but a forgery of any kind would be covered. The court rejected that construction, and found that the fraudulent emails were not financial instruments.

The Computer Fraud grant applied to unauthorized entry into the insured's computer system, and the introduction of instructions that propagated themselves through that system. The court applied the plain meaning rule to hold that (1) sending an email does not constitute unauthorized entry into a system, because the policy was designed to cover matters like the introduction of malicious code, and (2) the emails did not propagate themselves through the computer system.

Finally, the Funds Transfer Fraud grant encompassed "fraudulent … electronic … instructions issued to a financial institution directing such institution to transfer … money … from any account maintained by the [insured] at such institution, without the [insured's] knowledge or consent." The court found that the coverage was inapplicable because the insured knew about the transfers (it had requested them). The court also held that the receipt of emails purportedly from the insured's client to the insured does not trigger coverage because the insured was not a financial institution.

The lower court had found for Federal on the grounds that the insured's loss was not "direct." The Ninth Circuit did not address this ground, but affirmed summary judgment on other grounds. Thus it left the lower court's holding on the additional point undisturbed.

Georgia Federal District Court Holds There is No Computer Fraud Coverage for a Loss Enabled by a Coding Error

InComm Holdings, Inc. v. Great American Ins. Co., 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017). The court found no coverage under a Computer Fraud policy for claims arising from a scheme involving a Prepaid Debit Card Plan.

The insured, InComm, was a debit card processor providing a service enabling customers to load funds onto prepaid debit cards issued by banks. Debit card holders purchased "chits" from retailers, such as CVS or Walgreens, for the amount of the chit plus a service fee. InComm's computers allowed debit card holders to request transactions on their account, including redeeming the chits to load funds onto their cards, using telephone voice commands or touch-tone codes. With the redemption, InComm would transfer funds to the banks. However, there was a coding error in InComm's computer system. If cardholders used more than one telephone simultaneously to redeem the same chit, they would be credited with multiples of the amount of the chit. In a well-organized scheme, a criminal ring redeemed 1,933 chits an average of 13 times, for a total of 25,553 unauthorized redemptions, with a total

value of $11,477,287. The scheme spread over 28 states, and many of the purported individual "holders" of the relevant debit cards were victims of identity theft.

Great American's policy provides coverage for Computer Fraud, insuring against "loss of …money … resulting *directly* from the *use* of any *computer* to fraudulently cause a transfer …." (Emphasis added.) Applying Georgia law, the court granted Great American's motion for summary judgment. First, it found that the wrongdoers did not use a computer to make the redemptions. They used a telephone. It said "[A] person thus 'uses' a computer where he takes, holds or employs it to accomplish something. That a computer was somehow involved in a loss does not establish that the wrongdoer 'used' a computer to cause a loss." It went on to hold that even if a computer *had* been used, the "loss" did not result "directly" from that use. Nor did it result "directly" from the initial fraudulent redemptions, because they did not automatically cause the transfer of funds. Instead, the "loss" did not occur until the funds held by the banks were used to pay sellers for purchases made by the wrongdoers. Rather, the loss occurred because InComm itself chose to make transfers to the banks, and it was that decision that resulted "directly" in the loss.

Michigan Federal Court Finds No Coverage under a Crime Policy for Social Engineering-induced Fraudulent Funds Transfer

American Tooling Center, Inc. v. Travelers Cas. and Sur. Co. of America, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017). The court held that the wire transfer of $800,000 to an erroneous bank account for a vendor was not covered under a Crime policy, because it was not a "direct loss" that was "directly caused by the use of a computer."

The insured is a tool and die manufacturer which outsources some of its work to other manufacturers, including one called Shanghai YiFeng Automotive Die Manufacture Co., Ltd ("YiFeng'). The insured sent an email to YiFeng, requesting copies of all outstanding invoices. The response came from a third party, which used a domain that was deceptively similar to YiFeng's. Instead of the correct "yifeng-**m**ould.com" domain, the fraudster used "yifenfg-**rn**ould.com." It directed transfer to a new bank account, and the insured sent the funds as directed.

The court applied Michigan law to construe language that required a "direct loss" that was "directly caused by the use of any computer." The court found that there were intervening events – verifying that production milestones had been met, authorizing the transfers, and initiating the transfers without verifying bank account information. Also, fraudulent emails do not constitute "the use of any computer to fraudulently cause a transfer", and there was "no infiltration or 'hacking' of [the insured's] computer system." Thus, there was no direct loss.

New Jersey Federal Court Finds No Coverage for Reverse Social Engineering Loss under a Crime Policy for Lack of Ownership by the Insured

Posco Daewoo America Corp. v. Allnex USA, Inc., et al., 2017 WL 4922014 (D.N.J. Oct. 31, 2017. The court granted a Rule 12(b)(6) motion to dismiss a claim for loss through "reverse social engineering," because the funds lost when a customer was fraudulently induced to wire funds to erroneous accounts were never property owned by the Insured.

The Insured imports and exports chemicals, and supplied chemicals to Allnex, for which Allnex owed payment. An impostor posing as an employee of the Insured sent fraudulent emails directing payment to bank accounts controlled by the impostor. Without confirming the authenticity of the fraudulent emails or the accounts, Allnex wired the funds. The insured sued Allnex, and also its own insurer, Travelers, seeking indemnity for the loss caused by the imposter. Travelers had issued a Wrap and Crime Insurance Policy covering "direct loss" (which was an undefined term) from Computer Fraud, defined as "the use of any computer to fraudulently cause a transfer of money." It limited the property covered to property that the Insured owns or leases.

Applying New Jersey law, the court focused on the ownership requirement. The Policy did not define "own," but the court looked to the dictionary definition, and found the funds erroneously transferred on account of a debt were never owned by the Insured. Thus the court found no coverage, and did not need to reach the issues of whether there was a "direct loss" from Computer Fraud.

Decision Finding Coverage

New York Federal Court Finds Coverage under a Crime Policy for Social Engineering-induced Fraudulent Funds Transfer When a Computer Code Is Used to Alter Emails

Medidata Solutions, Inc. v. Federal Insurance Co., 2017 WL 3268529 (S.D.N.Y. July 21, 2017). In a case contrary to the prevailing trend, the court, applying New York law, held that the wire transfer of $4.8 million resulting from fraudulent social engineering was covered under a crime policy.

Medidata provides services to scientists conducting clinical trials. Although it has its own email domain address, it used Google's Gmail platform for company emails. Messages to employees were routed through Google servers for processing and storage. Gmail displayed the sender's full name, email address and picture in the "From" field of a message. A fraudster embedded a computer code in false emails, which caused certain Gmail messages to appear as if they came from Medidata's president. The emails directed an employee to make the transfer, and provided the name of a fictitious attorney who communicated with the employee in a telephone call. Ultimately, several senior officers approved the transfer.

The court concluded that this sequence of events constituted "deceitful and dishonest access," which the New York Court of Appeals had indicated would trigger computer fraud coverage in *Universal v. Am. Corp. v. Nat'l Union Fire Ins. Co.*, 25 N.Y.3d 675 (2015). The *Medidata* court held that such access fell within the language in the Computer Fraud coverage grant which defined a covered Computer Violation as "the fraudulent: (a) entry of Data into or deletion of Data from a Computer System" or "(b) change to Data elements or program logic of a Computer System, which is kept in machine readable format." It was sufficient that "[A] thief sent spoofed emails armed with computer code into the email system that Medidata used."

The court also concluded that these events fell within the Funds Transfer Fraud coverage grant of the Crime Policy, which defined Funds Transfer Fraud as "fraudulent electronic … instructions … purportedly issued by an Organization, and issued to a financial institution directing [a transfer] without such Organization's knowledge or consent." It reasoned that "the accounts payable personnel would not have initiated the wire transfer, but for, the third parties' manipulation of the emails." The court addressed the requirement that the transfer be "without such Organization's knowledge or consent" by saying that the "high level employees' knowledge and consent … was only obtained by trick" and that "larceny by trick is still larceny."

It bears note that the policy did not contain language requiring a "direct loss" or "directly caused by computer fraud" that is commonly found in Crime policy computer fraud endorsements. The case is on appeal to the Second Circuit.

Data Breach Decisions

Overview

The law continues to develop, erratically, on what kinds of claims can be brought against a company following a data breach. There have been claims based in tort, contract, various statutes, and equity. There have been conflicting results across states, and even within states. So the outcome depends on a case specific analysis of the particular claims and the applicable state law. Very broadly, plaintiffs have had more success in California and the Pacific Northwest than elsewhere.

Claims based on negligence allege either (1) breach of an alleged duty to maintain adequate data security, or (2) misrepresentations or fraud based on written statements. The statements can be made in Codes of Business Conduct, Privacy Policies, and Privacy Statements on Websites, or they can be sent with other documents, such as insurance policy descriptive booklets.

These *same* documents can be used to support claims of breach of contract, breach of implied contract, or breach of implied contract terms.

There have also been claims of negligence *per se*, on the theory that a violation of Section 5 of the Federal Trade Commission Act constitutes negligence on its face. And there have been claims based on violations of state Unfair and Deceptive Trade Practice Acts and other statutes, as well as federal statutes.

The claims can be brought by customers of companies that suffered a data breach, or by employees of those companies, or by policyholders of insurance companies that have been breached. They can also be brought by financial institutions which suffered losses from the breach.

The decisions may arise in motions to dismiss on the pleadings, and where they allow actions to proceed, they do not reflect final determinations on the merits. Others are motions to dismiss on the merits, and are dispositive, subject to appeals.

There are related issues concerning whether certification as a class action is appropriate. And two decisions addressed the application of privilege and work-product protection to post-breach forensic reports.

Some of these decisions also address the issue of federal standing, and these are discussed again in the final section of this review.

Claims Relating to Data Breaches

Decisions Dismissing Actions in their Entirety

Eighth Circuit Finds Article III Standing but No Viable Causes of Action for Breach of Securities Brokerage Firm's Network

Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. Aug. 21, 2017). The Eighth Circuit found standing where plaintiff alleged a breach of contract, regardless of its merits, but dismissed an action for failure to allege claims for breach of express and implied contract, unjust enrichment, and violation of a consumer protection statute.

Hackers breached the internal database of Scottrade, Inc., a securities brokerage firm, and acquired personal identifying information of over 4.6 million customers. They exploited the information to operate a stock manipulation scheme, illegal gambling websites, and a Bitcoin exchange. Putative class actions were consolidated, and dismissed by the district court for lack of Article III standing.

On appeal, the Eighth Circuit first reversed the lower court and found that plaintiff had standing. A further analysis of its reasoning appears in the portion of this Paper specifically addressing standing, below.

The court went on to decide a motion to dismiss for failure to state a claim which had been fully briefed below, but not decided by the district court in view of its determination

on standing. The Eighth Circuit dismissed plaintiff's claim for breach of express contract, which asserted that Scottrade's Privacy Statement stated that it used security measures that complied with federal law, including secured files and buildings, and it used Secured Socket Layer encryption. The court found these were representations of conditions that are in the nature of contract recitals, for which the appropriate claim was fraud in the inducement. No such claim was pled. The court went on to say that even if the representations were promises of contract performance, plaintiff did not identify *any* specific applicable law and regulation breached. A promise that Scottrade would not be hacked could not be plausibly implied. Further, there was no plausible allegation of actual damage, as the complaint did not allege anyone suffered fraud or identity theft resulting in financial loss. Payments for services were made on a per order basis, so the court found the allegation that a portion of the fees were for data management and security was not plausible. The court wrote that "[M]assive class action litigation should be based on more than allegations of worry and inconvenience."

The court dismissed claims for breach of implied contract and unjust enrichment because plaintiff did not identify the specific security measures Scottrade failed to undertake. The unjust enrichment claim also failed because under Missouri and Florida law (one of which controlled, the court said, without deciding which one), there can be no recovery for unjust enrichment when an express agreement covers the same subject matter.

The court also dismissed claims under the Missouri Merchandising Practices Act, a state consumer protection statute. Allegations of "fraudulent and deceptive acts" were not pled with sufficient particularity. Although merchandise can include services, Scottsdale did not sell data security services. Finally, the complaint did not identify how failing to discover and notify customers of the data breach was an unfair or deceptive trade practice.

Pennsylvania Intermediate Appellate State Court Finds No Duty to Protect Employee Information from a Data Breach

Dittman v. UPMC, 154 A.3d 318, 2017 WL 117652 (Pa. Super. Ct. Jan. 12, 2017). The Pennsylvania Superior Court affirmed the dismissal of claims against an employer resulting from a breach of electronically-stored personal and private information.

The University of Pittsburgh Medical Center (UPMC) suffered a data breach exposing information about its 62,000 present and former employees. At least 788 of those employees were subsequently victims of tax fraud. The employees asserted that UPMC breached a legal duty to protect their information, specifically by failing to properly encrypt data, establish adequate firewalls, and implement adequate authentication procedures. The court held that no such legal duty existed.

The court applied the Pennsylvania test to determine whether a duty exists, which requires consideration of five factors. The first factor is the relationship between the parties. Although the employer-employee relationship traditionally includes duties by

employers, and thus this factor weighed in favor of imposing a duty, the court did not view this as controlling. The test goes on to weigh two further factors, which are the "social utility of the actor's conduct" and "the nature of the risk imposed and foreseeability of harm incurred." The court concluded that while a data breach is generally foreseeable, that possibility does not outweigh the social utility and efficiency of storing information electronically. This balancing weighed against imposing a duty on UPMC. (The court strongly implied that if there had been allegations of specific threats and problems with UPMC's computer system before the breach occurred, the balancing might have come out differently.) The fourth factor is the consequences of imposing a duty. The court stated there was no need to further incentivize companies to protect confidential information, and recognized that companies would be required to incur potentially significant costs to increase security measures even though it is not possible to prevent data breaches altogether. It concluded that this factor weighs in favor of not imposing a duty. The final factor is the public interest in imposing a duty. Here the court accepted the trial court's view that because the legislature has specifically addressed data breaches, and has required only that notice be provided, the public interest would not be served by "judicial action that disrupts that [legislative] deliberation process." It also stated that creating a duty would "greatly expend judicial resources." Thus it found this factor weighed against creating a duty.

In addition, the court held that the economic loss doctrine prevented recovery in tort for solely economic damages unaccompanied by physical injury or property damage. Finally, the court held that there was no implied contract to protect the information, because there were no objective manifestations of intent to enter into such a contract, nor was any consideration paid.

Pennsylvania Federal District Court Dismisses Contract Claims against Employer in Data Breach

Enslin v. The Coca-Cola Co., 2017 WL 1190979 (E.D. Pa. Mar. 31, 2017). The court rejected claims that Coca-Cola had contractual duties to protect a former employee's personal data.

An IT employee of Coca-Cola took home laptop computers that were no longer in use, keeping some and giving others away. Some of those were previously used by HR personnel, and thus had personal information of 74,000 current and former employees. A few months after being notified of the breach, some of the plaintiff's accounts with online retailers were compromised. The plaintiff asserted that the company's employment application, its Code of Business Conduct, and two detailed information technology policies gave rise to a contractual duty to protect his information. Both sides moved for summary judgment.

The plaintiff was a member of the Teamsters Union, so as a preliminary matter, the court had to conclude that the collective bargaining agreements with the Teamsters did not pre-empt state law claims or subject plaintiff to a grievance procedure which he did not follow. It reached this conclusion because neither collective bargaining agreement

contained any terms relating to the safeguarding of personal information. The court held that portions of the Code of Conduct did create enforceable obligations, but none of the provisions in it or the policies or the employment agreement constituted a promise on the part of the company to safeguard personal information. Nor would the court imply such a term. It also declined to find an implied contract to safeguard personal information, citing to a Third Circuit case and to ***Dittman v. UPMC*** (see discussion above).

The court also rejected an unjust enrichment claim seeking restitution under the "opportunistic breach" theory, based on its earlier conclusion that there were no relevant contractual duties to breach.

Previously, in 2015, the court had dismissed, on the pleadings, plaintiff's claims for negligence, negligent misrepresentation, fraud, bailment, civil conspiracy, and violation of the Driver's Privacy Protection Act of 1994.

Illinois Federal District Court Dismisses Claims that Did Not Cause Economic or Out-of-Pocket Damages under Illinois and California Statutes, and Dismisses Action

In re Barnes & Noble PIN Pad Litigation, 2017 U.S. Dist. LEXIS 97161 (N.D. Ill. June 13, 2017). The court dismissed a Second Amended Consolidated Class Action Complaint for failure to state a claim under F.R.Civ.P. 12(b)(6). The data breach was perpetrated by PIN pad skimmers. The decision focused on whether plaintiffs had incurred economic or out-of-pocket damages, as required under the Illinois Consumer Fraud and Business Practices Act, the California Unfair Competition Act, and Section 1798 of the California Civil Code (ruling that the kinds of injury that will ground a 1798 claim are coextensive with such claims under the Unfair Competition Act). The court held that alleged injuries arising from the loss of the value of personal identifying information, time spent with bank and police employees, and emotional distress are not injuries sufficient to state a claim. It also held that plaintiff's temporary inability to use their bank accounts is also insufficient, because that is not a monetary injury in itself. The court held that the loss of cell phone minutes in speaking to bank employees was *de minimis* and too attenuated to be a redressable injury. And it held that the purchase of credit monitoring was insufficient under the applicable statutes, even if the data breach was the sole reason to renew credit monitoring services. (In this case, plaintiffs did not even allege it was the sole reason.) Concluding that plaintiffs had not alleged other injuries that would give rise to claims for relief, despite ample opportunities, the court dismissed the entire case.

Illinois Federal District Court Dismisses Breach of Contract Claim from Data Breach, Finding a Privacy Pledge Was Not Part of an Insurance Contract

Dolmage v. Combined Ins. Co. of America, 2017 U.S. Dist. LEXIS 185346 (N.D. Il. Nov. 8, 2017). The court found that a Privacy Pledge contained within the documents

accompanying an insurance policy is not incorporated by reference into the policy and is not a legally enforceable promise.

Combined offered insurance products to the employees of Dillard's department store. Plaintiff obtained a supplemental life insurance policy from it. Thereafter, Combined mailed to Plaintiff a package containing the insurance policy and 15 other documents described as "fulfillment materials." One of them was a Privacy Pledge making statements about the handling of its insureds' personal data. A third-party vendor of Combined placed files with the personal information of Plaintiff and other Dillard employees and their dependents on an unsecured location on its website. A fraudulent tax return was filed in Plaintiff's name, and Plaintiff commenced this action. After multiple rounds of motions to dismiss, the court was left to consider only the claim for breach of contract based upon alleged breach of the Privacy Pledge.

Applying Iowa law, the court rejected the contention that the Privacy Pledge was a "rider or endorsement" to the policy. It relied in large part on an expert report, not with respect to the expert's legal conclusions, but with respect to the background information on insurance compliance and drafting practices, and whether the Privacy Pledge was filed with the relevant state insurance authorities. It was not persuaded that the Privacy Pledge was not approved by insurance regulators was controlling, but did "not find it entirely irrelevant that it was not filed." The court also found it significant that the Privacy Pledge was not clearly marked in the header as a rider or endorsement, as is customary for actual riders and endorsements. Based on these factors, it concluded that "the Privacy Pledge did not create a legally enforceable promise."

Illinois Federal District Court Dismisses a Full Range of Claims and the Entire Action

Community Bank of Trenton v. Schnuck Markets, Inc., 2017 U.S. LEXIS 66014 (S.D. Ill. May 1, 2017). Financial Institution plaintiffs in a putative class action sued a chain of grocery stores that had experienced a data breach. The court dismissed all claims on a motion pursuant to F.R.Civ.P. 12 (b)(6), finding that plaintiffs failed to state a plausible claim for relief.

The court dismissed claims for negligence, gross negligence, and negligence *per se* under Missouri law. It stated that it was "not persuaded that public policy concerns, the existence of industry standards, or implied contractual relationships should give rise to a duty in this case." It noted that this breach took place during an early period of widespread data breaches, when many retailers were caught unaware, and "the law did not contemplate harms of the kinds that emerged." The court found that the Missouri data breach notification law does not contemplate a duty or remedies for anything other than a failure to notify, and gives the Missouri Attorney General the exclusive power to prosecute violations. It distinguished, on various grounds, prior holdings arising from the data breaches of Home Depot, Target, and BJ's.

The court also held that Section 5 of the FTC Act does not give rise to a duty and claims for negligence, and in any event, creates no private cause of action.

The court dismissed claims based on breach of implied contract under Missouri and Illinois law. It noted that the retailer, its banks, Visa and MasterCard had explicit contracts and duties to each other, but declined to "stretch those preexisting relationships and agreements to impliedly include Plaintiffs." Similarly, it denied claims that plaintiffs were third-party beneficiaries, referring to plaintiffs' allegations that that they received interchange fees or interest related to transactions as a "peripheral benefit."

The court dismissed claims asserting violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, stating that a claim under that Act must be based on more than a simple breach of contract, that no public policy had been violated, and that the "issuing banks [were not] being lured into authorizing transactions on the basis that defendant's data security was top notch." It also noted that the consumers were "apparently reimbursed for the trouble," which might also defeat this claim.

Finally, the court dismissed the unjust enrichment/assumpsit claim because "shoppers … did not pay more for groceries via card than they would with cash, so it cannot be said Defendant made more than it should have for those particular groceries."

Ohio Federal District Court Dismisses Claims for Violations of FCRA and Negligence, and Denies Leave to Add Statutory Claims

Galeria v. Nationwide Mut. Ins. Co., and ***Hancox v. Nationwide Mut. Ins. Co.,*** Case 2017 WL 4987663 (S.D. Oh. Aug. 16, 2017). In related putative class actions, the court dismissed claims under the Fair Credit Reporting Act ("FCRA") and for negligence, and denied leave to amend to add claims under Ohio and Minnesota statutes.

In the course of purchasing or seeking to purchase insurance from Nationwide, plaintiffs provided personally identifiable information. The information was stolen by hackers who made their way into portions of Nationwide's computer network. The case was heard on remand after an appellate court found that plaintiffs had standing to assert claims under the FCRA.

Addressing the merits of the FCRA claim, the court assumed without deciding that Nationwide qualifies as a consumer reporting agency under the Act. Plaintiffs alleged both willful and negligent violation of the FCRA as a result of an alleged failure "to adopt and maintain reasonable procedures to limit the transmission of consumer reports," and that Nationwide thereby "furnished" credit reports. The court found that being hacked did not constitute the affirmative act of furnishing reports, so it dismissed and denied leave to further amend the FCRA claim on the basis of futility.

The court also held that under Ohio law, the claims for negligence failed to meet causation requirements, even though one of the plaintiffs alleged that there had been

three unauthorized attempts to open credit cards in his name. However, these attempts did not occur until 15 months after the data breach. To the court, mere allegations of time and sequence were insufficient to prove causation, given the length of the time gap. It dismissed and denied leave to further amend the negligence claim on the basis of futility.

The court also denied leave to add claims for statutory violations. With respect to the Ohio Consumer Sales Practices Act, the court held the Act exempts insurance companies acting in their capacity as insurers, as Nationwide was acting here. Plaintiffs also sought to add a claim under the Minnesota Insurance Fair Information Reporting Act, which prohibits an insurer from disclosing personal or privileged information without authorization. The court concluded the theft of information by hackers would not constitute a "disclosure" under the Act.

Federal District Court Dismisses Claim of Bailment of Personal Data

Galeria v. Nationwide Mut. Ins. Co., and ***Hancox v. Nationwide Mut. Ins. Co.,*** Case 2017 WL 6375803 (S.D. Oh. Dec. 13, 2017). Bringing an end to the Nationwide cases, late in the year the court granted a motion under Fed.R.Civ.P. 12(b)(6) motion and dismissed a claim sounding in bailment.

The court found that under Ohio law, bailment exists where one person delivers personal property to another for a specific purpose, with the expectation it will be returned. Here, there was no delivery because there was no actual or constructive full transfer. Although Plaintiffs provided personal data, they never relinquished control of it. Under the circumstances, the concept of returning the property had no application.

Decisions Allowing Actions to Proceed

California Federal Court in Yahoo Data Breach Case Finds Standing and Allows Contract and Many Statutory Claims to Proceed

In re Yahoo!, Inc. Customer Data Sec.Breach Litig., 2017 WL 3727318 (N.D. Ca. Aug. 30, 2017). The case arose from the three massive data breaches between 2013 and 2016 compromising 1.5 billion accounts. In a consolidated class action, and on a motion to dismiss under Fed.R.Civ.P. 12(b)(6), the court allowed claims for breach of contract, unjust enrichment, and breach of the implied covenant of good faith and fair dealing to proceed. It allowed several statutory claims to proceed, and where it did not, it almost always granted leave to amend the complaint. It dismissed negligence claims based on forum grounds.

There are four putative classes: the first consisting of all Yahoo account holders in the United States; the second consisting of all account holders in Israel; the third consisting of all account holders in Australia, Venezuela and Spain; and the fourth consisting of all Small Business Account holders in the United States.

As a threshold matter, the court addressed Article III standing, and found that standing had been established. A further analysis of its reasoning appears in the portion of this Paper specifically addressing standing, below.

The facts were colored by allegations that Yahoo was especially lax in its attention to security measures, and that it delayed notice in several instances so as not to derail its takeover by Verizon.

The essential substantive allegations revolved around statements in Yahoo's Privacy Policy that said: (1) "[W]e are committed to ensuring your information is protected and apply safeguards in accordance with applicable law;" (2) "[Y]ahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under [certain inapplicable circumstances];" (3) "[W]e limit access to personal information about you to employees who we reasonably believe need to come into contact with that information to provide products or services to you in order to do their jobs;" and (4) "[W]e have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you." The Privacy Policy was incorporated via hyperlink into Yahoo's Terms of Service. Plaintiffs alleged that Yahoo breached these by failing to have reasonable safeguards in place, specifically in its data encryption protocol.

Plaintiffs asserted a breach of contract claim based on the statements in the Privacy Policy and Terms of Service. Yahoo relied on disclaimers and Limitations of Liability provisions for punitive, indirect, incidental, special, consequential or exemplary damages in its Terms of Service. The court allowed the claim to continue notwithstanding these provisions, save for the claims for out-of-pocket mitigation damages. But as to those, the court granted leave to amend, with the observation that plaintiffs "may be able to allege that the limitations…are unconscionable."

The court also allowed a claim for implied breach of contract to proceed, because it was pled in the alternative. Here, it treated out-of-pocket mitigation expenses the same way as in the express breach claim. It allowed the claim for breach of the implied covenant of good faith and fair dealing to proceed because plaintiffs alleged Yahoo engaged in bad faith "through this conscious awareness of and deliberate indifference to the risks to Class Members' PII by failing to take commercially reasonable steps to safeguard Plaintiffs PII."

Negligence claims were asserted only by the Australia, Venezuela and Spain class. The court dismissed these based on forum selection clauses.

Claims for declaratory relief were dismissed because plaintiffs did not identify contractual provisions to support their allegations that such provisions were "unconscionable and unenforceable, or precluded by federal and state law." The court afforded plaintiffs leave to amend.

Plaintiffs also asserted claims under several statutes: the California Unfair Competition Law; the California Consumer Legal Remedies Act; the California Customer Records Act; the California Online Privacy Protection Act; and the federal Stored Communications Act. The decision is a methodical, painstaking and meticulously-reasoned 93-page opus. In short, the court allowed many of the key statutory claims to proceed, and struck others, but allowed leave to amend the pleadings for almost all of the claims it struck. The only exceptions were claims under the California Customer Records Act made by non-residents of California, because residency is an express requirement of that statute, and all claims under the California Online Privacy Protection Act, which does not afford a private right of action.

Pennsylvania Federal District Court Allows Financial Institutions to Press Negligence, Negligence Per Se, and State Statutory Claims against Wendy's

First Choice Fed. Credit Union v. The Wendy's Co., 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017). On a motion to dismiss on the pleadings, the court adopted the report and recommendation of a magistrate, allowing claims brought by 26 financial institutions to proceed against Wendy's in connection with the data breach it suffered from hackers in 2015 and 2016.

As an initial matter, the magistrate was asked to make a choice of law ruling because of differences in the application of the economic loss doctrine. Wendy's urged for Ohio law, its home state, but plaintiffs urged that the laws of their various principal places of business should apply. This contest related to whether the loss of computer data can be considered property under the economic loss doctrine. The magistrate found that "it is not implausible that computer data could be considered property in this context," and thus it was plausible that the economic loss doctrine might not apply, so the magistrate declined to undertake a choice of law analysis at the early stage, prior to discovery.

Plaintiffs alleged specific acts and omissions in safeguarding payment card data, which the magistrate concluded were sufficient to advance a plausible claim for negligence. Plaintiffs also alleged that the failure to use reasonable measures to protect data and to comply with applicable industry standards violated Section 5 of the Federal Trade Commission Act and similar state statutes, and thus constituted negligence per se. Relying on and applying a 2016 ruling to that effect in the Home Depot data breach litigation, the magistrate allowed these claims to proceed. Plaintiffs further alleged that Wendy's violated the Ohio Deceptive Trade Practices Act by misrepresenting its security, and that they were damaged as a direct and proximate result. The magistrate took these allegations as sufficient to plead reliance, and ruled that these claims were plausible enough to proceed.

Finally, the magistrate declined to dismiss claims seeking declaratory and injunctive relief, because the claims assert continuing action by Wendy's, and found that the financial institutions could rely on the associational standing of their members to seek such relief.

In Premera Data Breach Case, Oregon Federal District Court Allows Some Tort and Contract-based Claims to Proceed, Dismisses Others

In re Premera Blue Cross Customer Data Sec. Breach Litig., 2017 WL 539578 (D. Or. Feb. 9, 2017). This is a putative class action alleging various state common law tort, contract, and statutory claims under Washington and Oregon law. Premera is a healthcare benefits servicer and provider which suffered a breach of its network, compromising the Personal Information of 11 million current and former members, affiliated members, and employees. Premera moved to dismiss the pleadings under Fed.R.Civ. P. 9(b).

As to the tort-based claims, plaintiffs alleged that Premera's policy booklets, Privacy Notice, and Code of Conduct contained affirmative misrepresentations under the Washington Consumer Protection Act ("WCPA"). The court observed that Washington law does not require reliance, and proximate cause is an issue of fact. It held that one of the booklets, the "Preferred Select" policy booklet, contained sufficiently specific representations that Premera would "make sure" that information remained secure, and plaintiffs alleged that the statement was false because Premera did not "make sure" the information was protected, but rather knew it had inadequate data security measures. However, even though the "Preferred Bronze" policy booklet stated that Premera "takes care" to ensure that information remains confidential by having a company confidentiality policy and by requiring all employees to sign it, Plaintiffs did not allege that Premera did not have such a policy or did not require its employees to sign it. Thus the court found that the allegations relating to that policy were insufficient to allege affirmative misrepresentation.

Premera's Privacy Notice contained various alleged misrepresentations on data security. These included Premera's commitment to maintain confidentiality, stating it took measures to comply with federal and state privacy laws, limiting authorized access to personal information, securing buildings and systems from unauthorized access, employee training, and protecting the information of former members. The court found that these representations, if false, were sufficient to support a claim of affirmative misrepresentation, so it allowed claims to stand as to plaintiffs who were provided with the Privacy Notice.

Premera's website contained a Code of Conduct, and Premera argued that certain statements on it were not deceptive because they were mere "puffery" or expressions of corporate optimism. The court found that the statements had the capacity to deceive and thus were sufficient to support a claim for deceptive statements under the WCPA.

The court found the plaintiffs did not allege facts demonstrating the tort of active concealment, so it dismissed those claims. However, it allowed the claims sounding in fraud by omission to stand. It found plaintiffs alleged that Premera should have disclosed that it did not implement industry standard access controls, did not fix known vulnerabilities in its electronic security protocols, failed to protect against reasonable anticipated threats, and otherwise did not comport with its assurances regarding

protecting information. Finally, plaintiffs argued that their allegations that Premera's conduct was unfair under the WCPA, were not subject to federal pleading requirements. The court disagreed, holding that those allegations were based upon deceptions, so federal pleading requirements applied, and were met (or not) according to its earlier rulings.

As to the contract-based claims, using the factual analysis it used for the tort claims, the court held that claims were sufficiently pleaded for breach of express contract by policyholders who were sent the Preferred Select policy booklet, but not the Preferred Bronze policy booklet, and for plaintiffs who received the Privacy Notice. The statements in the Code of Conduct, which were found to be sufficiently "deceptive" under the WCPA, were held not to be enforceable promises sufficient to support an express breach of contract claim.

The court found that for contracts governed by Washington law, there was no basis for a claim of breach of an implied contract term that adequate data security measures would be taken. However, for those contracts governed by Oregon law, it *was* appropriate to imply such a term. It rejected Premera's argument that implying a data security term would frustrate the purpose of Congress in not allowing a private right of action under HIPAA.

Plaintiffs also alleged the existence of implied-in-fact contracts for the provision of data security, separate from any express contracts. The court allowed this claim to proceed by policyholder plaintiffs, but dismissed it as to non-policyholder plaintiffs. It reasoned that because the overall contractual relationship necessarily required the provision of sensitive information, it was a plausible inference that plaintiffs understood and intended that Premera would adequately protect that information.

Finally, Premera sought to dismiss the claims on the grounds they are completely preempted under ERISA. Plaintiffs had identified specific provisions in the policy booklets and other documents that they allege were incorporated into their health benefits contract. Section 502(a) of ERISA allows civil enforcement claims to be brought by a participant (1) to recover benefits under the plan, (2) to enforce his rights under the terms of the plan, or (3) to clarify rights as to future benefits under the plan. The court found that data security was not an ERISA "benefit", so the only claims that might constitute ERISA claims were those "to enforce rights under the terms of the plan," because those claims were not limited to "benefits." However, the court found that although there is some relationship between data security and the administration of the ERISA plan, it was insufficient to overcome the presumption against preemption of state law, so plaintiffs' claims were not preempted.

Washington Federal Court Allows Negligence and Claims based on Washigton Data Breach and a Consumer Action Statutes to Proceed

Veridian Credit Union v. Eddie Bauer LLC*,* 2017 WL 5194975 (W.D. Wa. Nov. 9, 2017). The court addressed a motion to dismiss claims against retailer Eddie Bauer

("Bauer"). It allowed claims to proceed alleging negligence, violation of a Washington Statute specifically addressing cyber breaches which cause damage to financial institutions, and violation of the Washington Consumer Protection Act. In each claim, the allegations that Eddie Bauer failed to take reasonable care to employ adequate security measures provided a sufficient basis to proceed.

Hackers accessed Eddie Bauer's POS systems and installed malware affecting every Eddie Bauer store in the U.S. and Canada. They stole credit and debit card data and sold it to others who used the data for fraudulent transactions. Veridian issued payment cards and suffered financial losses in covering customers' losses and reissuing cards. It commenced a putative class action against Eddie Bauer.

Veridian argued that Washington law applied, because Eddie Bauer's corporate headquarters are there, so its alleged failure to employ adequate security measures was "orchestrated and implemented" there. Eddie Bauer argued for application of Iowa law because Veridian and most of its customers are located there. Applying the "most significant relationship" test, the court applied Washington law, concluding that the location of the alleged wrongful conduct carried the most weight because the location of the alleged injury was in multiple states and was fortuitous.

The court dismissed with prejudice the claim for negligence *per se* because Washington does not recognize it as a separate cause of action. On the basic negligence claims, the court found there was no special relationship between Veridian and Eddie Bauer, that Eddie Bauer owed no common law duties to Veridian to employ adequate security measures, and that Section 5 of the FTC Act was not designed to protect Veridian because it is neither a customer nor competitor of Eddie Bauer. However, the court allowed the case to proceed under a Washington statute, RCW 19.255.020, which was specifically designed to protect financial institutions that have incurred actual costs because of a party's failure to take reasonable care to guard against unauthorized access to payment card information. Indeed, the statute expressly so provides. The court found that the reasonable care standard established a minimum standard of conduct supporting a negligence claim under Washington law.

The court also allowed a claim based directly on violation of RCW 19.255.020, which requires that actual costs be related to payment card holders who are Washington residents. Although Veridian did not specifically allege it reissued cards to Washington residents, the court found it reasonable to infer that it did so in the context of a putative nationwide class action.

The court also allowed a claim under the Washington Consumer Protection Act to proceed, finding the alleged failure to take reasonable security measures constituted an unfair act which knowingly and foreseeably put Eddie Bauer's customers and payment card financial institutions at risk.

Finally, the court dismissed claims for declaratory and injunctive relief because they are requests for relief and not separate legal causes of action. It left leave to amend if and when plaintiff succeeds on a substantive cause of action warranting those remedies.

California Federal District Court Finds Standing and Allows Implied Contract, Negligence and Statutory Unfair Competition Claims to Proceed

Walters v. Kimpton Hotel & Restaurant Group, LLC, 2017 WL 3727318 (N.D. Cal. Apr. 13, 2017). Ruling on a motion to dismiss, the court found that a plaintiff who had been a guest at a hotel chain that suffered a data breach had asserted plausible claims in implied contract, negligence, and violation of the California Unfair Competition Law.

Hackers allegedly accessed Kimpton Hotels' computer systems across the U.S. The court found that because plaintiff was a guest during the at-risk window, it was plausible to infer that his payment card information was stolen.

The court allowed a claim to proceed that alleged the existence of an implied contract arising from Kimpton's privacy policy, which states that Kimpton is "committed" to safeguarding customer privacy and personal information. It found that plaintiff had suffered actual damages, including having to secure and maintain credit monitoring services and out-of-pocket expenses, and the value of time reasonably incurred to remedy or mitigate the breach. Next, the court allowed the negligence claim to proceed, merely noting that plaintiff had suffered actual damages. The court also ruled it lacked sufficient information to dismiss based on the economic loss doctrine at this stage. Third, it allowed claims for unfair and unlawful business practices under the California Unfair Competition Law to proceed, again because the plaintiff alleged economic injury. However, it dismissed a claim under the statute based on fraud because plaintiff had failed to plead reliance on Kimpton's alleged misrepresentations.

The court also found that plaintiff had standing. A further analysis of its reasoning appears in the portion of this Paper specifically addressing standing, below.

Decision Denying Class Certification for Data Breach

Illinois Federal District Court Denies Class Certification Based on Lack of Commonality in Governing Law and Damages

Dolmage v. Combined Ins. Co. of America, 2017 WL 1754772 (E.D. Ill. May 3, 2017). Plaintiff was an employee of a department store whose health insurer suffered a data breach. She alleges that the insurer failed to keep her personally identifiable information private. She originally pled many state and federal law claims, but after two rounds of motions to dismiss, only a state law breach of contract claim survived. That was based on the "Privacy Pledge" that was sent to insureds with the fulfillment documents.

The court denied plaintiff's motion for certification of a class consisting of all current and former employees of the department store, as well as their dependents. The court found that one of the key issues was whether the Privacy Pledge was part of the contract with insureds, and if so, what duties it imposed on the insurer. The proposed class covered individuals living in approximately 30 states, and the court concluded that this meant the class did not meet the commonality requirement for certification, because many different state laws would control the individual contracts issues. It also concluded that there was no commonality because determining whether each class member suffered a "resulting injury" would require a highly individualized inquiry. For example, it noted that some of the victims had suffered identity theft and experienced actual theft of funds; others may have encountered employment and relationship issues as a result of identity fraud; others may have only suffered credit-monitoring and other remediation expenses; and others may or may not have suffered emotional distress. The court went on to find that the additional requirement of typicality was not met, first because of the differences in state law, and next because the plaintiff suffered identity theft and claimed actual damages, but most proposed class members did not suffer. Upon denying the motion for class certification, the court ended its opinion by stating that "the parties are directed to exhaust all settlement possibilities in light of this opinion."

Decisions on Privilege / Work-Product Protection of Forensic Reports

Federal Court in Oregon Orders Production of Documents Relating to Post-Breach Remediation Report where the Work Began Before the Breach

In re Premera Blue Cross Customer Data Sec. Breach Litig. 2017 WL 4857596 (D. Or. Oct 27, 2017). The court declined to protect documents relating to a remediation report prepared by the cyber forensics firm Mandiant. In October 2014, Premera retained Mandiant to review Premera's data management system. On January 29, 2015, Mandiant discovered malware. On February 20, 2015, Premera hired outside counsel. On February 21, 2015, Premera shifted supervision of Mandiant's work to outside counsel, but did not otherwise change the scope of the work. Mandiant subsequently issued a report.

The court held that there was only one investigation performed by Mandiant, which began at Premera's request before the breach. Thus the insertion of outside counsel in the course of the investigation did not provide a blanket shield protecting the report and related documents from production. However, Premera would not be required to produce specific documents or portions of documents: (1) prepared for the purpose of communicating with an attorney for the provision of legal advice, and thereby privileged; (2) containing the mental impressions of counsel prepared in anticipation of litigation; (3) containing communications to counsel to provide factual information so counsel can prepare for litigation; or (4) involving a factual investigation done solely at the behest of counsel for litigation and no longer under the scope of the original work for which Mandiant was retained.

Federal Court in California Protects Documents Relating to Post-Breach Investigation and Report from Production

In re Experian Data Breach Litig., 2017 U.S. Dist. LEXIS 162891 (C.D. Ca. May 18, 2017). The court allowed Experian to withhold from production documents concerning a post-breach investigation and report issued by Mandiant.

In September 2015, Experian learned that one of its systems had been breached. It immediately retained Jones Day, its outside litigation counsel. Jones Day then retained Mandiant to conduct an expert report analysis. That report was not shared with Experian's Incident Response team. On these facts, the court had no difficulty concluding the investigation was conducted and the report was prepared in anticipation of litigation, and thus was protected by the work-product doctrine. It reached this conclusion even though Experian had independent business duties to investigate the breach, and even though Mandiant had previously worked for Experian in matters separate from this particular data breach. Plaintiffs contended Mandiant must have had access to Experian's live servers at the time of the breach, so the substantial hardship exception would apply if its reports were withheld. Experian submitted evidence that Mandiant did not have access to any of Experian's live systems, networks, or servers during its investigation, but rather only observed sever images. The court found that plaintiffs could obtain those same server images though discovery, and conduct their own review of them, so it rejected their claim of substantial hardship.

Decisions on Article III Standing Relating To Data Breaches

Overview

A significant recurring issue is Standing, which refers to whether a plaintiff has been sufficiently injured to bring a lawsuit in federal court, under Article III of the Constitution. Here, the federal circuits have split. They have interpreted and applied two key U.S. Supreme Court cases.

The first is ***Clapper v. Amnesty International, USA, et al.,*** 133 S. Ct. 1138 (2013), which involved warrantless wiretapping and was brought by various groups -- including reporters who thought they were being surveilled, or thought they might be surveilled. The Court held that for claims of future injury, there is no standing where the injury is "too speculative to satisfy the well-established requirement that threatened injury must be *certainly impending*" (emphasis added). Also, plaintiffs cannot manufacture standing merely by incurring expenses (such as flying to interview sources, rather than interviewing them by phone).

The other key case is ***Spokeo v. Robins*****,** 136 S. Ct. 1540 (2016), which held that "standing requires an actual or imminent, concrete and particularized injury-in-fact***,*** and

that a plaintiff does not "automatically satisfy the injury-in-fact requirement whenever there is a violation of a statute granting a statutory right, and purporting to authorize that person to sue to vindicate that right."

In data breach cases, the key issue is whether, following a data breach, the increased likelihood of future identity theft, in and of itself, is a sufficient harm. There is a split of authority. The D.C., Sixth, Seventh and Ninth Circuits have recognized that it does establish standing, but the First, Third, Fourth and Eighth Circuits have rejected that. In late 2017, a petition for certiorari was filed with the Supreme Court in the ***Attias v. CareFirst*** case, discussed below.

Some 2017 decisions found standing on other grounds.

Decisions Finding Standing

D.C. Circuit Finds Standing Based Solely on Increased Risk of Identity Theft following a Cybercrime

Attias v. CareFirst, Inc. 865 F.3d 620, 2017 WL 3254941 (D.C. Cir. Aug. 1, 2017). The D.C. Circuit ruled that an increased risk of future identity theft, without more, is sufficient to confer standing.

CareFirst is a health insurer which suffered a hack in 2014, revealing patients' names, birthdates, email addresses, social security numbers, and credit card information. Allegedly some of the data was unencrypted. The damages claimed were heightened risk of future identity theft. The court addressed the injury in fact requirement of standing, which requires the injury to be concrete, particularized, and actual or imminent. The court construed *Clapper, supra*, and *Susan B. Anthony List*, *supra*, as holding that the injury in fact requirement can be met if the injury is *either* "certainly impending" *or* there is a "substantial risk" that the injury will occur. The court then focused on whether the formulations in the pleadings sufficiently alleged a "substantial risk." Parsing through the inartful complaint, the court concluded that the complaint alleged the theft of social security or credit card numbers. To the court, it was sufficient that an unauthorized party had accessed personal data, and "to infer that this party has both the intent and ability to use that data for ill." Thus, "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." It held that the "fairly traceable requirement" does not require that the defendant be the most immediate cause, or even a proximate cause, of the injuries. Assuming that CareFirst failed to secure the data, the court had "little difficulty concluding that their injury in fact is fairly traceable to CareFirst." Finally although recognizing self-imposed mitigation costs do not fulfill the injury in fact requirement, the court found that they can satisfy the requirement that the injury be redressable.

The court remanded to the district court to address an antecedent question that remained unaddressed, namely whether the district court properly had diversity jurisdiction.

Plaintiffs also sought injunctive relief under the Administrative Procedures Act. The court declined to grant that relief because the complaints had not established that there was a sufficient likelihood plaintiffs would be subject to future breaches.

Eighth Circuit Holds Risk of Future Identity Theft Does Not Confer Standing, but an Allegation of Credit Card Fraud Following a Data Breach Does

In re SuperValu, Inc., 870 F.3d 763 (8th Cir. Aug. 30, 2017). The Eighth Circuit dismissed plaintiffs who merely alleged an increased risk of future identity theft. However, it permitted the action to proceed because one plaintiff alleged he had been the victim of credit card fraud following the breach.

The retail grocery chain SuperValu, Inc. suffered two hacks in 2014, allegedly revealing customers' names, credit or debit card numbers, expiration dates, CVV codes, and PINs. Plaintiffs in a consolidated class action alleged that SuperValu did not use best practices and industry standards for merchants because it used default or easily guessed passwords, failed to lock out users after several failed login attempts, and did not segregate access to different parts of its network or use firewalls. They alleged an "imminent and real possibility of identity theft**,"** relying on a 2007 GAO report on data breaches. One of the plaintiffs, David Holmes, incurred a fraudulent charge on his credit card, which he cancelled and replaced.

The court applied the tests in *Clapper v. Amnesty Int'l USA,* 568 U.S. 398 (2013) and *Susan B. Anthony List v. Driehaus,* 134 S. Ct. 2334 (2014) that plaintiffs alleging future injury must demonstrate "the threatened injury is 'certainly impending' or there is a 'substantial risk that the harm will occur.'" It found that the GAO report did not plausibly support the contention that consumers affected by a data reach face a substantial risk of credit or debit card fraud. It rejected the argument that costs incurred to mitigate the risk of identity theft constitute an injury in fact for purposes of standing. "[T]he time plaintiffs spent protecting themselves against this speculative threat cannot create an injury."

Although allegations of future injury were insufficient to confer standing, the court found that Holmes, the plaintiff who alleged a present injury, had standing. The court found that credit card fraud is a form of identity theft. It found that the misuse of the card met the test of being "fairly traceable" to the defendant's alleged breaches. A putative class action can proceed as long as one plaintiff has standing. Because Holmes had standing, the court allowed the class action to proceed. It did, however, dismiss the remaining plaintiffs who merely alleged an increased risk of identity theft.

Eighth Circuit Finds Article III Standing where a Party Alleges Breach of Contract, Regardless of the Merits of the Claim

Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. Aug. 21, 2017). The Eighth Circuit applied the test established by the U.S. Supreme Court in *Spokeo, Inc. v. Robins,* 136 S. Ct. 1540 (2016), which required that to establish standing, a plaintiff must have an injury that is "concrete and particularized and actual or imminent, not conjectural or hypothetical." The plaintiff alleged a breach of contract on the theory that a portion of the fees paid to Scottrade were used to meet contractual obligations to provide data security and protect his information. He asserted that the difference between the amount paid and the value of services received is an actual economic injury that established injury in fact. The court applied previous Eighth Circuit authority holding that "a party to a breached contract has a judicially cognizable interest for standing purposes regardless of the merits of the breach alleged." Thus it found plaintiff had standing.

Third Circuit Holds that Alleged Violations of the Fair Credit Reporting Act Concerning Disclosure of Personal Information through a Data Breach Are Sufficient to Establish Article III Standing

In re Horizon Healthcare Serv., Inc. Data Breach Litig. 846 F.3d 625, 2017 WL 242554 (3rd Cir. Jan. 20, 2017). The Third Circuit held that with the passage of the Fair Credit Reporting Act (FCRA), Congress established that the unauthorized dissemination of personal information by a credit reporting agency in and of itself causes an injury sufficient to establish Article III standing.

Two laptops containing unencrypted personal information of more than 839,000 Horizon members were stolen. Plaintiffs in a putative class action alleged willful and negligent violations of the FCRA. There were no allegations that identities were stolen as a result of the breach. (Although one plaintiff alleged he was the victim of a fraudulent tax return and a denial of credit, the court did not reach his argument.)

The court found there was no doubt that plaintiffs had alleged a particularized injury, because they alleged the disclosure of their own private information. Thus, the court only addressed the concreteness requirement of the injury in fact element of standing. It recognized established authority that the violation of a statute creating legal rights can cause an injury in fact sufficient for standing. The court held that with the passage of the FCRA, Congress established that the mere unauthorized dissemination by a credit reporting company causes an injury, even though the information is truthful and not harmful to anyone's reputation. It stated that Congress provided for damages for willful violations, which shows that Congress believed that FCRA violations cause concrete harm. That is, Congress "elevated the unauthorized disclosure of [credit] information into a tort."

The court rejected arguments that *Spokeo, Inc. v. Robins,* 136 S. Ct.1540 (2016) compelled a different outcome. It concluded that *Spokeo* did not create a requirement

that plaintiffs show that a statutory violation has caused a "material risk of harm" to establish standing.

There are separate issues of whether Horizon is a "consumer reporting agency" subject to the FCRA, and whether the FCRA applies when data is stolen rather than voluntarily furnished. Those are subject to another motion on which the district court had not ruled, so they were not yet before the appellate court.

California Federal Court in Yahoo Data Breaches Finds Standing Based on Increased Risk of Future Identity Theft

In re Yahoo!, Inc. Customer Data Sec. Breach Litig., 2017 WL 3727318 (N.D. Ca. Aug. 30, 2017). Following its own cases and Ninth Circuit authority, the court concluded that all plaintiffs had suffered an injury in fact because all had an increased risk of future identity theft. It also accepted the alternative argument that plaintiffs had suffered an injury in fact due to the loss in the value of their PII. It also found injury in fact for plaintiffs whose PII had already been misused by identity thieves, those who had paid out of pocket mitigation expenses, and those who alleged a loss of benefit of the bargain.

California Federal District Court Finds Standing Based on Loss of Data through Hack

Walters v. Kimpton Hotel & Restaurant Group, LLC, 2017 WL 1398660 (N.D. Cal. Apr. 13, 2017). Hackers allegedly accessed Kimpton Hotels' computer systems across the U.S. The court found that because plaintiff was a guest during the at-risk window, it was plausible to infer that his payment card information was stolen. In a breathtakingly superficial analysis, the court concluded that plaintiff had standing, because he plausibly alleged "that his data had already been stolen and that it was taken in a manner that suggests it will be misused."

Decisions Finding No Standing

Fourth Circuit Holds that Increased Risk of Future Identity Theft Does Not Establish Article III Standing

Beck v. McDonald, 848 F.3d 262 (4th Cir. Feb 6, 2017). The Fourth Circuit affirmed a district court's holding that allegations of an increased risk of identity theft are insufficient to establish the non-speculative, imminent injury in fact required for Article III standing.

The court consolidated cases involving two breaches at a Veteran Affairs Medical Center. The first involved the likely theft of an unencrypted laptop with personal information of over 7,400 patients. The second involved the loss or theft of four boxes of pathology reports containing identifying information and medical diagnoses of 2,000

patients. The plaintiffs alleged violations of the Privacy Act of 1974 and the Administrative Procedure Act.

The court focused on the injury in fact element, and found that "threatened injury'" was not "certainly impending" as required by *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). It also rejected plaintiffs' claims that "emotional upset" and "fear [of] identity theft and financial fraud" are adverse effects sufficient to confer standing. The court acknowledged a difference in federal circuits, noting that (at the time) the Sixth, Seventh, and Ninth Circuits have recognized, at the pleading stage, that the threatened injury of identity theft can establish an injury in fact, but the First and Third Circuits have not. It stated, however, that in the cases finding standing (at the time), there were allegations that pushed the threatened injury of future identity theft beyond the speculative to the sufficiently imminent. For example, those cases involved hackers who intentionally targeted personal information, and in one there was an allegation of specific misuse of the information. No such allegations were made in the present case, rendering the risk of future identity theft too speculative. The mere theft of a laptop and boxes did not indicate that the private information had been targeted or accessed.

In addressing a potential second basis for standing, the court declined to find a "substantial risk" that harm will occur, leading a party to reasonably incur mitigation or avoidance costs. It also declined to follow other circuits which inferred a substantial risk of future identity theft from an organization's offer to provide free credit monitoring services. And it held that any mitigation expenses incurred by the plaintiffs were "self-imposed harms [that] cannot confer standing."

Second Circuit Finds Unsuccessful Attempted Charges Following Stolen Credit Card Information Do Not Establish Standing

Whalen v. Michaels Stores, Inc., 689 Fed.Appx. 89, 2017 WL 1556116 (2nd Cir. May 2, 2017) (Summ. Order). The Second Circuit affirmed a dismissal for lack of standing in a case alleging exposure of credit card information, but no other personal data. The retailer Michael's suffered a breach in 2014. Shortly after plaintiff made purchases at Michael's, there were two attempts to make charges to the card in Ecuador. She cancelled her card, and no charges were actually incurred. The card was subsequently cancelled. No other personally identifying information was alleged to have been stolen. Although she alleged she lost time and money resolving the attempted fraudulent charges and monitoring her credit, she provided no specifics. On these facts, the court found no injury in fact and hence no standing. Note that this was a Summary Order, and therefore has no precedential effect, although it may be cited.

Federal Court in District of Columbia Finds No Standing against the U.S. Government for Claims Relating to the Office of Personnel Management ("OPM") Breach

In re: U.S. Office of Personnel Mgmt. Data Sec. Breach Litig. 2017 WL 4129193 (D.D.C. Sept. 19, 2017). The court dismissed claims under the federal Privacy Act

(which controls information practices for federal agencies), the Little Tucker Act (which gives federal courts jurisdiction over certain contract claims of less than $10,000 against the U.S.), and the Administrative Procedures Act for lack of standing. It also dismissed the claims under Fed.R.Civ.P. 12(b)(6) for failure to state a claim.

Four breaches of the OPM computer network led to the acquisition of sensitive data of over 21 million people. This included information obtained in the course of conducting background investigations for people seeking jobs with various levels of security clearances. Some plaintiffs allege they experienced actual identity theft or credit card fraud. They all allege risk of future identity theft and other harm associated with that risk. The court found no standing for either the individuals or trade unions. It rejected arguments that the release or theft of private information is itself an injury-in-fact, in the absence of actual or threatened misuse of the information.

The court distinguished the D.C. Circuit Appeals Court decision in *Attias v. CareFirst*, 865 F.3d 620 (D.C. Cir. 2017) (discussed above), on the grounds that *Attias* arose out of a cyberattack on a health insurance company, and the *Attias* court found that "a substantial risk of harm already exists, simply by virtue of the hack and the nature of the data." To the *OPM* court, "standing in *Attias* was predicated on the slender thread that one could fairly assume what the thieves meant to do with the stolen information." No plaintiff who alleged actual harm alleged that credit card numbers or accounts had been compromised in the hack, and the government forms collecting information did not ask for account-identifying information.

Moreover, although no official attribution of the source of the breach has been made, the court noted that the complaint alleged the breaches were widely reported to have been perpetrated by the Chinese government. The U.S. House of Representatives Committee on Oversight and Government reform reached the same conclusion. The court stated that the fact the OPM breach "arose out of a particular sort of cyberattack against the United States, differentiates it from the majority of the legal precedent that arises in the context of retail establishments or other financial entities." While not reaching the issue of whether the Chinese government in fact was responsible for the breaches, the court noted that the circumstances rendered it unable to rely on the presumption that informed the *Attias* court. It said "the *Attias* court based its decision on a particular cybercrime in a commercial setting – 'the hack and nature of the data that plaintiffs allege was taken' – and it did not purport to address every data breach, including those that might be state-sponsored."

Some plaintiffs allege they are already victims of identity theft or financial fraud, and two had out-of-pocket expenses which actually rectified the fraud or identity theft (as opposed to cautionary expenses, such as credit monitoring). The court found that this constituted an injury-in-fact. However, the court also found that these plaintiffs had failed to allege causation. They did not plausibly connect the "various isolated incidents" to the breaches at issue. "Allegations that two things happened in sequence are not sufficient to show causation."

The court found additional reasons to dismiss the claims. The Privacy Act requires actual harm. But the two plaintiffs who allege actual harm failed to allege that OPM "disclosed" private information. As that statutory term has been defined by the courts, "disclosure" requires a transmission, but here the data was not transmitted by OPM. Rather, it was stolen. Also, plaintiffs did not plead sufficient facts to allege their losses were "as a result" of OPM's actions. Further, to constitute an "intentional or willful" violation of the Privacy Act, an agency's actions must be greater than gross negligence. The court found that allegations of omissions such as failure to patch, maintain a vulnerability scanning program, and continuously monitor a system would not establish that OPM acted in an "intentional or willful manner." And again, there were no allegations that the government had anyone's payment card numbers. So the Privacy Act claims were dismissed. The claims under the Little Tucker Act would have required an "express or implied contract" with the U.S. They were dismissed because plaintiffs had no such contract. The claims for declaratory and injunctive relief under the Administrative Procedures Act were dismissed because the Privacy Act expressly limits the categories for which such relief is available.

Claims that OPM violated a "constitutional right to informational privacy" were dismissed. The Supreme Court has assumed, but not expressly recognized, the existence of such a right. Lower appellate courts have touched on but not resolved the issue. The *OPM* court declined "to recognize a constitutional violation that no court has even hinted might exist: that the assumed constitutional right to informational privacy would be violated not only when information is disclosed, but when a third party *steals* it."

Finally, claims against a company that conducted background investigations for OPM were dismissed because it had derivative immunity as a government contractor.

Decisions on Article III Standing in Other Contexts

On Remand, Ninth Circuit Again Holds that *Spokeo* Plaintiff Has Standing under Fair Credit Reporting Act

Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. Aug. 15, 2017). In 2016, the Supreme Court remanded this case for a determination of whether an alleged violation of the Fair Credit Reporting Act (FCRA) constitutes a harm sufficiently concrete to satisfy the injury in fact requirement. On remand, the Ninth Circuit held the facts before it were sufficient to establish standing.

Plaintiff alleged that Spokeo, which compiles individual consumer information profiles, published an allegedly inaccurate report about him on its website. Plaintiff alleged that these errors harmed his employment prospects at a time when he was unemployed, that he continues to be unemployed, and suffers emotional distress as a consequence.

The FCRA provides a right to sue and recover statutory damages even in the absence of actual damages. The court observed that the mere fact that Congress says a consumer may sue does not mean that a federal court has power to hear the suit, if there is no standing. It adopted the formulation of the Second Circuit in *Strubel v. Community Bank,* 842 F.3d 181 (2nd Cir. 2016): "an alleged procedural violation [of a statute] can by itself manifest concrete injury where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents 'a risk of real harm' to that concrete interest." Applying that test, the Ninth Circuit found the FCRA provisions did protect consumers' concrete interests. "[T]he real world implications of material inaccuracies in [consumer] reports seem patent on their face." "[R]eputational and privacy interests … have long been protected in the law."

Having found there was a concrete interest, the court turned to whether the alleged violations actually create a "material risk of harm." It said that not "every minor inaccuracy reported in violation of FCRA" will qualify, citing the example of an incorrect zip code. But here, Spokeo falsely reported that plaintiff was married with children, employed in a professional or technical field, has a graduate degree, that his wealth is higher than it is, and that he is older than he is. The court agreed that information of this sort may be important to employers or others using a consumer report. "[E]ven seemingly flattering inaccuracies can hurt an individual's employment prospects as they may cause a prospective employer to question the applicant's truthfulness or to determine that he is overqualified for the position sought."

Finally, the court rejected the argument that the allegations of harm were too speculative to establish a concrete injury. Here, it focused on the fact that there is no issue of threatened conduct that might not occur. Rather, the materially inaccurate consumer report had in fact already been published.

Eleventh Circuit Holds that Mobile App User Has Article III Standing, but No Status as a Subscriber under Video Privacy Protection Act

Perry v. Cable News Network, Inc., 854 F.3d 1336 (11th Cir. Apr. 27, 2017). The Eleventh Circuit held that the user of a mobile app whose activities were shared without his consent had Article III standing, but yet had no cause of action for statutory relief under the Video Privacy Protection Act (VPPA).

Plaintiff downloaded the CNN App to his iPhone. Among other things, the App allows a user to view videos. Plaintiff alleges that without a user's knowledge or consent, CNN tracks the views, collects a record, and then forwards that information, together with the user's MAC address (which identifies the specific mobile device) to a data analytics company called Bango. Bango receives other information from an extensive range of networks and devices. As described by the court, "Bango is able to compile personal information, including the user's name, location, phone number, email address, and payment information, and it can attribute this information to a single user across different devices and platforms." Plaintiff alleged a violation of the VPPA, which

prohibits a video provider from the knowing disclosure of personally identifiable information of its renters, purchasers, or subscribers.

The court affirmed a decision granting a motion to dismiss on the pleadings, but first found that plaintiff had standing. The court found that the structure and purpose of the VPPA demonstrates that it provided a cause of action for "any person aggrieved." The court said the VPPA protected against a type of invasion of privacy, and such an invasion has long been recognized as a tort by the great majority of jurisdictions. Thus, the court concluded that such a wrongful disclosure by a video provider satisfies the concreteness requirement of Article III standing.

However, the court found that plaintiff lacked the necessary status as a subscriber. The court applied its earlier decision in *Ellis v. Cartoon Network, Inc.,* 803 F.3d 1251 (11th Cir. 2015), which held that downloading and using a free app does not make the user a subscriber under the VPPA. In refusing to allow an amended complaint, the court rejected plaintiff's argument that because CNN was part of his cable television package, plaintiff was a subscriber of CNN. It ruled that in the absence of an "ongoing commitment or relationship" with CNN, plaintiff is not a subscriber. Given this disposition, the court was not required to rule on whether a MAC address and video history were "personally identifiable information" under the VPPA.

January 4, 2018

Vince Vitkowsky is a partner in Seiger Gfeller Laurie LLP, resident in New York. He represents insurers and reinsurers in product development and coverage matters across many lines of business, including cyber, CGL, and professional liability. He also defends insureds in complex claims. Vince's Twitter account, @vince_vitkowsky, https://twitter.com/vince_vitkowsky?lang=en, concentrates on cyber risks, liabilities and insurance, and provides brief, timely updates on new cases. He can be reached at vvitkowsky@sgllawgroup.com. Information on Seiger Gfeller Laurie LLP can be found at www.sgllawgroup.com.