SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber and Privacy Coverage Litigation 2016

Vincent J. Vitkowsky

New York Connecticut New Jersey

SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber and Privacy Coverage Litigation 2016

Vincent J. Vitkowsky

There were several notable reported decisions concerning coverage for data breaches, privacy risks, and deceptive funds transfer losses in 2016. They arose under several different lines of coverage, and are summarized in this article.

Data Breach Claims Under Cyber Policies

Arizona Federal Court Rules that Cyber Insurance Policy Does Not Cover PCI Fees and Assessments

P.F. Chang's China Bistro v. Federal Ins. Co., 2016 WL 3055311 (D. Ariz. May 26, 2016). The court held that PCI fees and assessments were not insured under a CyberSecurity by Chubb Policy on the grounds that they fell within the exclusions for (1) liability assumed under any contract or agreement and (2) any obligation assumed with the consent of the Insured. The restaurant chain P.F. Chang's suffered a breach which led to the credit card information of 60,000 of the restaurant's customers being posted online. Chubb reimbursed Chang's for more than $1.7 million in breach-related costs. Chang's sought an additional $1.9 million, representing the costs of reimbursing Bank of America, the processing bank, under a Master Service Agreement. The court examined three separate items for which coverage was sought. First, it found that the Fraud Recovery Assessment did not fall within the insuring clause covering "Loss on behalf of an Insured on account of any claim first made against the Insured . . . for Injury." Injury was defined to include a Privacy Injury. The court reasoned that Bank of America did not sustain a Privacy Injury itself, and therefore could not maintain a valid claim for Injury against Chang's. Next, it found that the Operational Assessment Fee would have been covered as Privacy Notification Expenses, save for the exclusions. Third, it found that the Case Management Fee qualified as a covered Extra Expense, and thus might have been covered, although there was an issue of fact as to whether the Fee was paid within the Period of Recovery of Services. Despite the conclusions regarding the Operational Assessment Fee and the Case Management Fee, the court ruled that coverage for all three assessments was precluded by the exclusion for loss "based upon, arising from, or in consequence of any . . . liability assumed by any insured under any contract or agreement." Further, coverage was also precluded by the exclusion for "any costs or expenses incurred to perform any obligation assumed by, on behalf of, or

with the consent of any Insured." The claimed damages also fell outside the definition of Loss, which did not include "any costs or expenses incurred to perform obligation assumed by, on behalf of, or with the consent of any Insured." Finally, the court examined and rejected arguments that coverage existed pursuant to the reasonable expectations doctrine, dismissing the arguments as "merely attempts to cobble together such an expectation after the fact." The case is on appeal to the Ninth Circuit.

Tech E&O Claims Under Cyber Policies

Utah Federal Court Allows Case to Proceed on Claims Handling Issue, Despite Finding No Duty To Defend

Travelers Prop. Cas. Co. of Am. v. Federal Recovery Servs., Inc., 2016 WL 146453 (D. Utah Jan. 12, 2016). As reported in **Cyber and Privacy Coverage Litigation 2015**, last year a federal court applying Utah law ruled that Travelers had no duty to defend under the Tech E&O liability portion of its CyberFirst® policy for an insured's refusal to return certain customer information in connection with a merger. The complaint alleged no error, omission, or negligent act. Rather, it alleged that the Insured acted with "knowledge, willfulness and malice." Comparing the allegations in the complaint against the language of the policy, the court found that there could be no coverage and hence there was no duty to defend. *See Travelers Property Cas. Co. of Am. v. Federal Recovery Services, Inc.,* 103 F.Supp.3d 1297 (D.Utah 2015).

In early 2016, the court refused to dismiss a counterclaim against Travelers for breach of the implied duty of good faith and fair dealing. Initially, the insured forwarded notice of the action to its broker, who testified that Travelers told him not to file a claim until formal papers had been served. The court allowed the case to proceed on the "narrow issue" of whether requiring the filing of papers before investigating resulted in a dilatory denial, causing financial consequences to the insured. The court also revisited and confirmed its 2015 coverage determination. It addressed whether the duty to defend analysis was limited by the Eight Corners rule, thus prohibiting the consideration of extrinsic evidence. It construed the policy language "any claim or 'suit' seeking damages for loss to which the insurance provided . . . applies" to permit only an Eight Corners analysis. It contrasted that to language such as "we will defend an insured against any covered claim or suit," which would permit extrinsic evidence.

The case was voluntarily dismissed on March 15, 2016.

Data Breach and Privacy-Related Claims Under CGL Policies

Fourth Circuit Finds Duty To Defend Class Action for Data Breach Under CGL Policy

The Travelers Ind. Co. of Am. v. Portal Healthcare Solutions, L.L.C., 2016 WL 1399517 (4th Cir. Apr. 11, 2016). In an unpublished opinion, the Fourth Circuit affirmed a lower court decision finding a duty to defend a class action arising from a data breach of personal health information under the Coverage B Personal and Advertising coverage grant of a CGL policy. The class action complaint alleged that Portal engaged in conduct resulting in private medical records being available online for over four months by anyone with an Internet connection. The Fourth Circuit applied Virginia law and invoked the Eight Corners Rule (*i.e.,* analyzing the four corners of the complaint and the four corners of the policy to determine whether the claims were potentially covered). It concluded that the complaint at least potentially or arguably alleged that a "publication" of private medical information had occurred, and dismissed Travelers' "[E]fforts to parse alternative dictionary definitions [to] absolve it of the duty to defend." The court reached this conclusion despite an absence of proof that any third parties had actually viewed the private records or that Portal had intended to publish the information.

The Fourth Circuit's decision is contrary to the recent trend in cases finding no coverage for data breaches under CGL policies. *See, e.g., Recall Total Info. Mgmt., Inc., v. Federal Ins. Co.,* 317 Conn. 46 (2015) (finding no coverage under Coverage B where there was no evidence that a third party accessed the information or that any person suffered any damages) and *Zurich Am. Ins Co. v. Sony Corp. of Am.,* No. 651982/2011, 2014 WL 3253541 (N.Y. Sup. Feb. 24, 2014) (finding no coverage under coverage B where the alleged publication was not an intentional act committed by the insured, but rather the criminal act of a hacker). Arguably, the import of this decision may be limited because, as an unpublished opinion, it is not binding precedent. Finally, the policies were legacy policies without cyber exclusions.

Alabama Federal Court Finds No Duty To Defend or Indemnify for Data Breach Under Property and Liability Policy with Inland Marine Computer Endorsements

Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., 2016 WL 6217161 (N.D. Ala. Oct. 25, 2016). In a thorough and carefully reasoned decision, the court found no coverage for a data breach under various sections of a property and liability policy with Inland Marine Computer endorsements. Three credit unions sued a grocery store, alleging that its negligence led to a hack compromising confidential data on the credit unions' customers. They sought damages for the reissuance of cards, reimbursement of customers for fraud losses, lost interest and transaction fees, lost customers, diminished good will, and administrative expenses associated with investigating, correcting, and preventing fraud. Both the property and liability sections of the policy had definitions of "property" that did not include electronic data, and both had exclusions

for losses involving electronic data. There were two Inland Marine endorsements, which covered direct physical loss to computer equipment and removable data storage media, and accidental direct loss to computer programs, electronic data in a computer or on computer storage media, or electronic data supplied for processing or other use in the insured's business operations.

On summary judgment, the court found no duty to defend or indemnify. It found that the Inland Marine endorsements were first-party coverags that imposed no duty to defend or indemnify against *any* claims, notwithstanding that they provided the insurer may "elect to defend" suits from claims of owners of property. If found that the liability portion of the policy did not provide coverage because the underlying suit did not allege claims for bodily injury, property damage, or personal and advertising injury as defined in the policy, but rather sought recovery for purely economic loss. It rejected the argument the physical debit cards were tangible property, finding that even if they were, the damage claimed was not to the physical cards themselves, but rather to the intangible electronic data contained on the cards. Finally, it rejected the argument that combining the duty to defend from the liability portion of the policy and the first-party coverage for electronic data loss from the Inland Marine endorsements, created "an amalgamation providing liability insurance against claims for electronic data loss."

Second Circuit Rules Knowing Violations Exclusion Does Not Eliminate Duty To Defend Class Actions Alleging Sharing of Private Information

Nat'l Fire Ins. Co. of Hartford v. E. Mishan & Sons, Inc., 2016 WL 3079958 (2d Cir. June 1, 2016). Applying New York law, the Second Circuit held that insurers had a duty to defend class actions under the Personal and Advertising Injury coverage of their CGL policies, notwithstanding a "knowing violations" exclusion, because not all of the claims asserted included elements of knowledge or intent. The insured shared private customer information with a telemarketer, who allegedly attempted to trap customers into recurring credit card charges. The insured was sued in two class actions alleging statutory violations, fraud by omission, breach of contract, and unjust enrichment. It contended it was entitled to defenses from several insurers pursuant to the Personal and Advertising Injury coverage portion of its CGL policies. The insurers sought declaratory judgments that they had no duty to defend by virtue of the exclusion for injury from knowing violations of another's rights. The district court granted summary judgment for the insurers, but the Second Circuit reversed in a Summary Order. The Second Circuit reasoned that it could not conclude with certainty that there was no coverage, because conduct that would trigger the knowing violations exclusion was not an element of each cause of action alleged. Even though the plaintiffs in the class actions alleged that the insured acted knowingly and intentionally, the actual conduct they described did not rule out the possibility that the insured acted without knowledge or intent. Specifically, the causes of action for breach of contract and for unjust enrichment do not have elements of knowledge or intent. The breach of contract claim was precluded by another exclusion for breach of contract. However, the unjust enrichment claim was not excluded, and as a result, the insurers had a duty to defend the entirety of the class actions.

Missouri Federal Court Applying Illinois Law Finds No Duty to Defend Action Alleging TPCA Violations Because of Express Exclusions, Notwithstanding Additional Claims

Regent Ins. Co. and Gen. Cas. Ins. Co. v. Integrated Pain Management, SC, 2016 WL 5357408 (E.D. Mo. Sept. 23, 2016). Applying Illinois Law, the court found no duty to defend a suit brought under the Telephone Communications Protection Act ("TCPA"), applying express TCPA exclusions despite the existence of additional claims. A medical office sent unsolicited faxes. A proposed class action alleged both violations of the TCPA and claims for common law conversion of the recipients' fax machine, toner, paper, and employee time. Two of the insurers, whose policies contained express TCPA exclusions, moved for summary judgment. The court granted their motions, concluding that the TCPA exclusions also preclude coverage for claims arising out of the same conduct as the alleged TCPA violations. The court was also unpersuaded by the argument that some of the faxes were not advertisements, but rather held that all the claims fell within the exclusions as interpreted in Illinois case law.

Missouri Federal Court Finds No Duty To Defend or Indemnify a TCPA Suit Because of Unsolicited Communications Exclusion

***The Travelers Ind. Co. of Connecticut v. Max Margulis, et al.*,** Case. No. 4:15-cv-01706 (E.D. Mo. Dec. 15, 2016). Applying Missouri law, the court found no duty to defend or indemnify a suit brought under the TCPA by a person who received a call on his cell phone without his prior consent from a vacation resorts company using an automated telephone dialing system. It applied an "Unsolicited Communications" endorsement which bars coverage for claims arising out of any actual or alleged violation of any law restricting or prohibiting the sending, transmitting, or distribution of unsolicited communications. It found that alleged violations of the TCPA fell within this endorsement.

Data Breach Claims Under Business Owner's Policy

New York Appellate Division Denies Coverage for Data Breach Under Business Owner's Policy with Electronic Data Exclusion

RVST Holdings, LLC v. Main St. Am. Assurance Co., 137 A.D.3d 1196 (N.Y. App. Div. 3d Dept. 2016). An intermediate appellate court in New York found no coverage for a data breach under a Business Owner's policy containing an electronic data exclusion. A chain of fast food restaurants was hacked and its customers' credit card information was stolen and used. A bank sustained damages for reimbursing fraudulent charges and sued the chain for negligently failing to safeguard the information. The chain made a claim for indemnity and defense under its Business Owner's policy. The insurer denied, and after losing in the lower court, prevailed on appeal. The insurer relied on policy language that defined "property damage" as "physical injury to tangible property,"

and further provided that "electronic data is not tangible property." Also, the policy specifically excluded "damages arising out of the loss of . . . electronic data." Finding this language unambiguous, the appellate court found there was no coverage and hence no duty to defend. The court also ruled that the separate section of the policy providing coverage for property damage consisting of "direct physical loss of or damage to" the insured's own property did not apply to third-party claims.

Deceptive Funds Transfer Claims Under Crime Policies

Eighth Circuit Finds Coverage under a Financial Institution Bond For a Hacker's Fraudulent Wire Transfer Notwithstanding Employee Negligence

The State Bank of Bellingham v. BancInsure, Inc., 2016 WL 2943161 (8th Cir. May 20, 2016). The Eighth Circuit held that Bellingham, a small Minnesota bank, was entitled to coverage under a financial institution bond when a hacker broke into the bank's network and performed two fraudulent wire transfers, notwithstanding that the hack was enabled by employee negligence. The bank utilizes Federal Reserve's FedLine Advantage Plus system, which requires two bank employees to physically insert tokens into a desktop computer to effectuate wire transfers. An employee accidentally left a computer running overnight with the tokens inserted, and a hacker made two unauthorized transfers. The first transfer was successfully intercepted and reversed, but the second could not be, and the bank sought coverage for a loss of $485,000. The insurer denied coverage on the basis that the bank's employee had acted negligently in leaving the desktop running overnight with the tokens inserted, and the loss thus fell within an exclusion for employee-caused loss.

Minnesota law applied, and Minnesota has adopted the concurrent causation doctrine, which affords coverage when multiple causes contribute to a loss, even though one of the causes is excluded. The court rejected the argument that this doctrine did not apply to financial institution bonds, and that the standard of proof of causation was higher for financial institution bonds than for general insurance policies. Applying the test of whether the loss was "directly caused" by the employee's negligence, the court held that the "efficient and proximate cause" (the "overriding cause") of the loss was the transfer by the hacker, not the negligence of the employee. It thus affirmed summary judgment in favor of the bank.

Fifth Circuit Finds No Coverage under Crime Protection Policy for Social Engineering-Induced Deceptive Funds Transfer Because Email Was Not the Direct Cause of Loss

***Apache Corp. v. Great American Ins. Co*.,** -- Fed.Appx --, 2016 WL 6090901 (5th Cir. Oct. 18, 2016). Applying Texas law, the Fifth Circuit found no coverage for a social engineering induced transfer of funds under a Crime Protection Policy. The Computer Fraud provision insured against "loss . . . resulting directly from the use of any computer

to fraudulently cause a transfer of [money] from inside the premises." The fraudster made a telephone call to an oil production company, claiming to be an actual vendor, and requesting that future payments be sent to a new bank account. Upon being told the request had to be in made in writing, the fraudster sent an email from an email address that was similar to the vendor's, attaching a letter purportedly on the vendor's letterhead, providing both the old bank account transfer number and the new one. An Apache employee called the telephone number on the letter, and spoke with a person using the name of the person who usually dealt with invoices for the vendor. The Apache employee concluded the requested change was legitimate. A different Apache employee approved and implemented the change, and in response to invoices from the actual vendor, transferred millions of dollars to the fraudster's account. In finding there was no coverage, the court concluded that although the email was part of a scheme, it was merely incidental to the occurrence of the authorized transfer of funds. If Apache had conducted a more thorough investigation, such as calling the correct telephone number known from past communications, it would not have changed the account information.

Ninth Circuit Finds No Coverage under a Crime Policy Because Funds Transfer Was Made by Authorized User

Pestmaster Services Inc. v. Travelers Cas. and Surety Co. of America, 656 Fed.Appx. 332, 2016 WL 4056068 (9th Cir. July 29, 2016). Applying California law, the Ninth Circuit affirmed a district court in holding that there was no coverage for lost funds transferred by the insured to a payroll company, which failed to remit the portion representing payroll taxes to the IRS. It held that neither the Computer Fraud nor the Funds Transfer Fraud insuring agreements applied where the transfer is made by an employee who was an authorized user of the system. Also, "[B]ecause computers are used in almost every business transaction, reading [the Computer Fraud] provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy."

Washington Federal Court Finds No Coverage under a Crime Policy Because Funds Transfer Was Made By Authorized User

Aqua Star (USA) Corp. v. Travelers Cas. and Surety Co. of America, 2016 WL 3655265 (W.D. Wa, July 8, 2016). Applying Washington law, the court found no coverage for a hack of a vendor of shrimp. The hacker directed the vendor's customer, a seafood importer, to change the bank account to which it made wire transfer payments. An employee of the importer did this and the company lost $713,890. The court applied an exclusion providing that the Policy "will not apply to loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System." It found that the actions of an authorized employee in effecting the wire transfers were an indirect cause of the loss, so coverage was barred. The case is on appeal to the Ninth Circuit.

Georgia Federal Court Finds Coverage under a Crime Policy Because of Ambiguity in Language

Principle Solutions Group, LLC v. Ironshore Ind. Inc., 2016 WL 4618761 (N.D. Ga, Aug. 30, 2016). This case found coverage when an employee of the insured transferred $1.7 million as a result of a scheme in which a fraudster posing as an executive sent an email to the employee instructing her to make the transfer, but the specifics as to where to wire the funds were provided in a subsequent telephone call. The insurer argued that because of the intervening telephone call and the company employee's actions in setting up and approving the transfer, the loss was not covered. The policy provided coverage for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit [the insured's] 'transfer account' and transfer pay, or deliver 'money' or 'securities' from that account." The court found that this provision was ambiguous and should be construed in favor of the insured.

New York Federal Court Orders Discovery into Specifics of Intrusions Used to Effectuate Funds Transfer

Medidata Solutions, Inc. v. Federal Ins. Co., 2016 WL 7176978 (S.D.N.Y. March 10, 2016). This highly-watched case involves a loss of $4.8 million through a voluntary electronic transfer made by an authorized user of a computer system induced by a social engineering fraud. Both parties had moved for summary judgment. By Order dated March 9, 2016, the court denied both motions without prejudice due to an insufficient record. The fraud included fictitious emails purportedly sent from one employee of Medidata to another. Medidata seeks coverage under a crime policy providing coverage for losses resulting from Computer Fraud through a Computer Violation, defined as "fraudulent entry of data into . . . a Computer System" or a "fraudulent change of data elements . . . of a computer system." The insurer argues that coverage is precluded because there was no manipulation or unauthorized entry into a computer system, so there was no involuntary transfer effected by hackers, forgers or impostors.

The insurer placed heavy reliance on a 2015 New York Court of Appeals decision in *Universal Am. Corp. v, Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, 25 N.Y.3d 275 (2015). That case found no coverage under a Computer Systems Fraud Rider for losses resulting from the entry of fraudulent medical claims into a health insurer's computer system by authorized users. The New York Court of Appeals found the Rider was intended to cover deceitful and dishonest acts of outside hackers, not entries by authorized users. However, the Order in *Medidata* did not refer to *Universal Am*. Instead, in denying summary judgment to both parties, the court in *Medidata* granted leave to conduct expert discovery. The discovery is "to be limited to establishing the method in which the perpetrator sent its emails to [Medidata], and discussing what changes, if any, were made to [Medidata's] computer systems when the emails were received." If the case proceeds to a further decision, it could provide significant insight into the facts and analysis that would inform future computer-related coverage disputes.

Other Case of Note

Illinois Federal Court Refuses to Dismiss Case Alleging that an Insurer's Privacy Pledge Was Part of Its Policy

Dolmage v. Combined Ins. Co. of America, 2016 WL 754731 (N.D. Ill. Feb. 23, 2016). In the context of a motion to dismiss a putative class action on the pleadings, the court allowed the case to proceed on the basis of a claim for breach of contract, which alleged that an insurance company's Privacy Pledge was part of its insurance contract. Plaintiff was an employee of Dillard's department stores. Dillard's employees had health insurance through Combined Insurance Company of America. Combined's Privacy Pledge stated, among other things, that Combined "maintain[s] physical, electronic and procedural safeguards that comply with federal regulations to guard your personal information." It further stated that it would require its outside vendors to abide by the same privacy standards. Plaintiff alleges that a security failure by one of Combined's vendor's led to her personal information being posted online, and that she and 30 other Dillard's employees were victims of identity theft. The policy defines itself as "this policy with any attached applications(s) and any riders and endorsements." At this early stage of the case, only needed to apply liberal federal pleading standards. The court did not accept Combined's position that the Privacy Pledge could not possibly qualify as an endorsement or a rider. Plaintiff alleged that the Privacy Pledge was sent to her along with the policy documents, and the court was required to accept this allegation as true. Thus it found plaintiff's claim that the policy incorporated the Privacy Pledge is not implausible, so it allowed the case to proceed.

January 4, 2017

Vince Vitkowsky is a partner in Seiger Gfeller Laurie LLP, resident in New York. He represents insurers and reinsurers in coverage matters across many lines of business, including cyber, CGL, and professional liability. He also defends insureds in complex claims. Vince can be reached at vvitkowsky@sgllawgroup.com. More information on Seiger Gfeller Laurie LLP can be found at www.sgllawgroup.com.