SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks and Insurance Coverage Decisions 2018

Vincent J. Vitkowsky

New York Connecticut Boston New Jersey

SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks and Insurance Coverage Decisions 2018

Overview

The principal cyber risks in 2018 were ransomware, cyber extortion, network interruption, data breaches, lost data, cryptomining losses, and liability from websites and social media. In addition, fraudulent funds transfers have come to be thought of as a cyber risk.

Over the years, some key decisions have involved claims for network 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, either in practice or by express language. Some have actively marketed the fact that they provide coverage. Others go further. For example, some insurers introduced variants of a Cyber Optimal Recovery Endorsement to all-risk policies. 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 -- whichever 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 four – including one in 2018 – 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.***, No. CV-15-01322-PHX-SMM, 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. Since the policy in that case was issued, most cyber policies issued to companies within the PCI framework have been drafted to expressly address PCI-related payments.

Finally, there has been much litigation concerning coverage for fraudulent funds transfers, often but not always induced by social engineering, under crime policies. Insurers have successfully denied coverage in most cases, but in 2018, two federal circuit courts of appeal found for the insureds.

In 2018, there were nine noteworthy coverage decisions concerning cyber risks under various lines of business. Those are summarized below. The Paper concludes with a brief discussion of current cases involving a key emerging issue, the application of the War Exclusion to cyber risks.

Duty to Defend Computer Fraud and Abuse Act Claims under D&O Policy

Delaware Superior Court Finds Duty to Defend Action Alleging Employee Appropriation of Electronic Information, including Trade Secrets, because One Count Alleged Non-Specific Breach of Computer Fraud and Abuse Act

Woodspring Hotels LLC v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, No. N17C-09-274 EMD CLDD, 2018 WL 2085197(Del Super. Ct. May 2, 2018). An individual who changed employers appropriated electronic information, including a customer database, with the assistance of an IT consultant to the original employer. This resulted in litigation that was settled. The court granted Partial Summary Judgement on a claim for indemnity for defense costs.

The insurer objected to paying defense costs on the grounds that the policy excluded claims for misappropriation of trade secrets. Of the 11 counts in the underlying complaint, 9 mentioned trade secrets. Two did not. The first such count was based on the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. Sec. 1030(a). That federal statute prohibits accessing a computer without authorization or in excess of authorization, knowingly and with intent to defraud, and obtaining "anything of value." It does not require the item of value to be a trade secret or even confidential. The count did not mention trade secrets. The second such count was for civil conspiracy to violate the CFAA, arising from the role of the consultant in exfiltrating the information. It, too, did not specifically mention trade secrets.

The court based its ruling on either Kansas or Delaware law, having conducted an extensive analysis showing there was no conflict between the two. It concluded that on these facts, there might be coverage on at least the two counts implicating the CFAA, so it found that the insurer had a duty to defend.

Data Breach/PCI Coverage under Management and D&O Policy

Fifth Circuit Finds Duty to Cover Legal Fees in Action Against Payment Processor

Spec's Family Partners Ltd. v. Hanover Ins. Co., 739 Fed. Appx. 233 (5th Cir. 2018). The insurer issued a Private Company Management Liability Policy with a Directors, Officers and Corporate Liability Coverage Part 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. A federal district court in Texas found that an insurer had no

duty to pay legal fees in a case to recover receipts withheld by a payment processor following a data breach. The lower court applied the contractual liability exclusion. The Fifth Circuit reversed.

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 initially had paid the fees in this action pursuant to a Defense Funding Agreement. Hanover subsequently stopped paying the fees, on the theory that they were not defense expenses, but rather were incurred in pursuit of an affirmative claim against First Data.

Applying Texas law, the lower court concluded that the Merchant Services Agreement was the source of the claim, so the contractual liability exclusion applied. The Fifth Circuit disagreed. It applied the eight-corners rule (looking only at the four corners of the complaint or demand letters and the four corners of the policy). It held that the demand letters included references to "'non-complian[ce]' with third-party security standards and not insignificant demands for non-monetary relief, wholly separate from the Merchant Agreement." It concluded that the allegations "implicate theories of negligence and general contract law that imply Spec's liability for assessments separate and apart from any obligations" under the Merchant Agreement. Thus, the Fifth Circuit held that the insurer had a duty to pay legal fees in the action by the insured against the payment processor.

Data Breach and Cyber-related Privacy Coverage under CGL Polcies

Florida Federal District Court Finds No Duty to Defend Under CGL Personal Injury Coverage for Alleged Negligence Leading to a Data Breach by Hackers

St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc. and Rosen Hotels & Resorts, Inc., Case No. 17-cv-540-41GJK (M.D. Fla. Sept. 28, 2018), *appeal docketed*, No. 18-14427 (11th Cir. Oct. 19, 2018). Rosen Millennium, Inc. ("Millennium") provided data security services to Rosen Hotels & Resorts, Inc. ("RHR"). RHR suffered a data breach at one of its hotels, which it disclosed to potentially affected customers. RHR sent a demand letter to Millennium, indicating that RHR believed the data breach was caused by Millennium's negligence. Millennium submitted a notice of claim to its CGL insurer, which initiated a declaratory judgment action as to its duty to defend.

The demand letter specifically tracked the language defining "Personal Injury" as "an injury, other than bodily injury or advertising injury, that's caused by a personal injury offense." That in turn is defined to include "[m]aking known to any person or organization covered material that violates a person's right of privacy." The parties agreed that the term "making known" is synonymous with "publication." Applying

Florida law, the court found the only plausible interpretation of the policy is that the publication must be made by the insured. Here, it was not, but rather by third-party hackers. Thus, the court found there was no coverage and hence no duty to defend, and granted the insurer's motion for summary judgment.

Coding Exploit Fraud under Computer Fraud Policy

Eleventh Circuit Holds There is No Computer Fraud Coverage for a Loss Enabled by Fraudsters Exploiting a Coding Error, because the Loss Did Not Result Directly from the Exploit

Interactive Communications Int'l, Inc. v. Great American Ins. Co., 731 Fed. Appx. 929 (11th Cir. 2018). Affirming a federal district court in Georgia, the Eleventh Circuit found no coverage under a Computer Fraud policy for claims arising from a scheme involving a Prepaid Debit Card Plan. However, it affirmed on different grounds.

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.

The lower court had concluded that the fraudsters did not use a computer to perpetrate the fraud, but rather used a telephone, so there was no coverage. The Eleventh Circuit disagreed with that conclusion. The policy covered losses through "the [use] of a computer." The Eleventh Circuit found that the fraud involved ***both*** telephones and computers, and that telephones were used to manipulate – and therefore ***use*** – the computers.

However, the Eleventh Circuit still found no coverage because the policy requires the loss to "result[] directly from the computer fraud." It interpreted that language to mean that "one thing results 'directly' from another if it follows straightaway, immediately, and without any intervention or interruption." The court detailed four steps in the fraud: (1) the manipulation of computers; (2) the transfer of money by the insured to a bank; (3) a fraudulent cardholder making a purchase; and (4) the actual transfer of money from a bank to a merchant to cover the purchase. Step 4 was the point at which the insured

could not recover the money. The court found this chain was too remote to satisfy the "resulting directly" requirement.

Fraudulent Funds Transfers under Crime and Computer Fraud Policies

Decisions Finding No Coverage

Ninth Circuit Finds the Exclusion for Electronic Data Input by a Person with Authority Bars Coverage for Social Engineering Loss under a Computer Fraud Policy

Aqua Star (USA) Corp. v. Travelers Cas. and Sur. Co. of America, 719 Fed. Appx. 701 (mem) (9th Cir. 2018). Employees who were defrauded by social engineering authorized and sent four payments to a fraudster's account. The insured sought coverage under a Computer Fraud policy, and the insurer denied coverage.

In a three-page, not for publication opinion, the Ninth Circuit held for the insurer. Applying Washington law, it applied an exclusion which it said unambiguously provides that the policy "will not apply to loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System." Thus, the transfers made by employees were not covered losses.

Decisions Finding Coverage

Second Circuit Finds Coverage under a Crime Policy for Social Engineering-induced Fraudulent Funds Transfers When a Computer Code is Used to Alter Emails

Medidata Solutions, Inc. v. Federal Ins. Co., 729 Fed. Appx. 117 (mem) (2nd Cir. 2018) Summary Order. The Second Circuit affirmed a controversial decision of the S.D.N.Y. applying New York law, holding 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.

Medidata sought recovery, claiming that the losses stemmed from "entry of Data into" or "change to Data elements or program logic of" a computer system. The insurer

contended that the policy only applied to hacking-type intrusions. Applying New York law, the court concluded "the fraudsters … crafted a computer-based attack that manipulated Medidata's email system," which was a computer system. "The attack represented fraudulent entry of data into the computer system, as the spoofing code was introduced into the email system. The attack also made a change to a data element, as the email's appearance was altered by the spoofing code to misleadingly indicate the sender."

The court further found that the transfer of funds was a "direct loss," *i.e.,* the fraudulent emails were the proximate cause of the loss.

Sixth Circuit Finds Coverage under a Crime Policy for Social Engineering-induced Fraudulent Funds Transfer

American Tooling Center, Inc. v. Travelers Cas. and Sur. Co. of America, 895 F.3d 455 (6th Cir. 2018). The Sixth Circuit, reversing a Michigan federal district court, found coverage for a series of fraudulent funds transfers totaling $834,107.78 under a business insurance policy that included Computer Fraud in its Computer Crime part. It held that a Computer Fraud caused a direct loss.

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. (As described by the lower court, instead of the correct "yifeng-**m**ould.com" domain, the fraudster used "yifenfg-**rn**ould.com.") It directed transfers to a new bank account, and the insured sent the funds as directed. When a demand for payment by the actual vendor led to discovery of the fraud, the insured agreed to pay 50% of the outstanding debt, and that the remaining 50% would be contingent on the insurance claim.

The Sixth Circuit applied Michigan law to construe language that required a "direct loss" that was "directly caused by the use of any computer." On the issue of direct loss, the insured argued it was suffered the moment the wire transfers took place. The insurer argued it did not arise until the fraud was discovered and the insured agreed to pay at least half the amount owed to the vendor. The court noted a split in jurisprudence, which it described as dividing between cases holding (1) "direct" means immediate and (2) "direct" means immediate or proximate. However, it held that under either test, a direct loss was suffered the moment the funds were transferred.

The court further held that the conduct of the fraudsters constituted Computer Fraud. The policy defined that as "the use of any computer to fraudulently cause a transfer of Money … from inside the premises or Financial Institution Premises …. to a person … [or place] outside the Premises or Financial Institution Premises." The insurer argued that this language required hacking or some other improper access or control of the computer. The court rejected that, noting that the insurer could have limited the

definition of Computer Fraud along those lines but chose not to. Here, it was sufficient that fraudulent emails were sent using a computer, which fraudulently caused the transfers. It also held that the "direct loss" was "directly caused" by the Computer Fraud, because the Computer Fraud was the immediate cause of the loss.

The court also rejected the application of three exclusions. First, it rejected the exclusion for loss resulting from giving money in an exchange or purchase. The court found that the insured did not transfer any money to the fraudster in exchange for anything from him. It noted that the exclusion was "loosely worded" and construed it against the insurer. Next, the insurer relied on an exclusion for "the input of Electronic Data by a natural person having authority to enter the Insured's Computer System." The court rejected this because the definition of Electronic Data excludes "instructions or directions to a Computer System," and found the employee's entries implementing the transfers to be "instructions or directions." Finally, the insurer relied on an exclusion for fraudulent documents used as source documentation in the preparation of Electronic Data. The court rejected this on the grounds previously cited, that the employee's entries did not constitute Electronic Data.

Coverage for Theft of BitCoin under Homeowner's Policy

Ohio State Court Finds Theft of Bitcoin Covered as Loss of Property, Not Cash, and thus Not Subject to Sub-Limits

Kimmelman v. Wayne Ins. Grp., Case No. 18-cv-001041 (Ohio Misc. 2nd, filed Sept 25, 2018). Plaintiff submitted a claim under his homeowner's policy for $16,000 in stolen Bitcoin. The insurer paid $200, on the grounds that Bitcoin was "money" subject to a $200 sub-limit. It relied on references in the press to Bitcoin as money, and also to Internal Revenue Service Notice 2014-21, which refers to cryptocurrency as "virtual currency."

The court rejected this argument, based on the actual conclusion of IRS Notice 2014-21, which recognized Bitcoin as property and subject to taxation as property. It denied the insurer's motion for judgment on the pleadings.

Also of Interest: Email Content Scanning under CGL Policy

California Federal Court Finds Duty to Defend and Indemnify Yahoo! in Email Content Scanning Cases

Yahoo! Inc., v. National Union Fire Ins. Co. of Pittsburgh, PA, No. 5:17-c-00489-EJD, 2018 WL 4962033 (N.D. Cal. Oct. 12, 2018). Yahoo! tendered several class actions to its CGL insurer. Allegations included that Yahoo! "wiretapped or eavesdropped upon and/or recorded the e-mails of Plaintiffs and the Class sent from their non-Yahoo! accounts to the Yahoo! accounts of private individuals before receipt

by the Yahoo! subscriber without the consent of all parties to the confidential e-mail communication," and that Yahoo! scanned and analyzed "each and every email sent to Yahoo! Mail users, including those sent from non-Yahoo! users." There were allegations that Yahoo! profited and derived a "financial windfall" from these activities. The court found that the insurer had a duty to defend and indemnify in these actions.

The policy was a fronting policy. Yahoo! retained the risk of loss and generally agreed to indemnify the insurer. The policy provided the standard coverage for "personal injury," defined to include "[o]ral or written publication, in any manner, of material that violates a person's right to privacy." It did not have the standard exclusion for injury "committed by an insured whose business is … [a]n Internet search, access, content or service provider."

The court found that liability for personal injury requires the disclosure of private content to a third party. It found it "reasonably inferable" from the allegations of profiting that Yahoo! was disclosing the emails to third parties. Further, even though the policy had a criminal acts exclusion, there was a possibility of a claim for civil damages, which would give rise to coverage.

In respect of one of the actions, the insurer agreed to provide a defense two years after the tender. Yahoo! argued the insurer had breached its duty by delaying a defense. The insurer argued that the claims professional who issued the coverage denial was not the same one who examined prior lawsuits. The court found this irrelevant because the potential for coverage was apparent from the later complaint itself. Next, the insurer argued that Yahoo! did not provide it with the terms of the policy. (For reasons not made clear in the opinion, the insurer did not have a complete copy.) The court found no authority for the proposition that "an insurer's duty to defend is delayed during the time it operates under an incomplete copy of the policy it drafted."

The insurer, however, was entitled to enforce its rights under a Deductible Endorsement. Pursuant to that Endorsement, Yahoo! agreed to reimburse the insurer for any amounts paid as damages and any Allocated Loss Adjustment Expense ("ALAE"), which was defined to include "all fees for service of process and court costs and court expenses" and "attorneys fees." It also provided the insurer paid ALAE and "all expenses" as "Supplementary Payments." The court found that because this was a fronting policy, the policy should not be interpreted to give the insurer a risk that the insured agreed to retain. Thus, it gave effect to the Deductible Coverage Endorsement.

Turning to the duty to indemnify, the court arrived at mixed results. For two class actions dismissed without payment being made, there was no duty to indemnify, and hence no breach of that duty. It found that for an action settled while damages claims involving personal injury were still pending, there was a duty to indemnify. It also held that payment of class action attorney's fees to plaintiffs' counsel qualify as "damages" under the policy, as "sums that the insured becomes legally obligated to pay as damages" because of "'bodily injury' arising out of 'personal injury.'" The service awards to class representatives, however, did not qualify as "damages."

Finally, there was a claim for breach of the covenant of good faith and fair dealing. Among the assertions by the insured were, among other things: (1) in its denial, the insurer cited an exclusion for "Insureds in Media and Internet Type Businesses" which was not in the policy; and (2) it used an incomplete copy of the policy to determine coverage. The court held that whether the claims handling constituted bad faith should be made by the jury.

A Key Emerging Issue – War Exclusions

Increasingly, cyber attacks with commercial consequences have been initiated by nations or agents acting on their behalf. Also increasingly, other nations make official attributions of these attacks. For example, the U.S., U.K., Canada, Australia, and New Zealand attributed 2017's WannaCry attack to North Korea. Also in 2017, an extremely destructive attack given the name Petya/NotPetya spread from a corrupted software update at small firm in Ukraine to the systems of major industrial companies around the world, causing massive losses. It was a combination of ransomware and wiperware, permanently destroying data and wiping hardrives. The U.S. and the U.K. officially identified Russia as initiating the attack.

Typical war exclusions not only extend to traditional wars, but to other circumstances, such as "hostile or warlike actions," whether war is declared or not, and others, depending on the specific exclusion. Cyber insurance policies have often simply taken the language of war exclusions from policies in other lines of business, and those other lines typically make no distinctions between kinetic and cyber perils.

There is no public indication that cyber insurers have relied on war exclusions to contest coverage for WannaCry, Petya/NotPetya, or other losses. However, at least two actions have been commenced against all-risk property insurers who have invoked war exclusions in connection with the Petya/NotPetya attack.

In ***Mondelēz Int'l, Inc. v. Zurich American Ins. Co.,*** Cir. Ct., Cook County, IL, No. 2018L011008, filed Oct. 10, 2018, Mondelēz alleges the attack rendered 1700 of its severs and 24,000 of its laptops permanently dysfunctional, and caused more than $100 million in losses. Its policy with Zurich covered "all risks of physical loss or damage" to its property, including "Physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction …." It also provided TIME ELEMENT coverage for the period during which the insured's electronic data processing equipment or media failed to operate. The war exclusion applied to "hostile or warlike action in time of peace or war." In addition to alleging that the incursions of malicious code did not constitute "hostile or warlike action," Mondelēz alleges that the exclusion "is vague and ambiguous, particularly given Zurich's failure to modify that historical language to specifically address the extent to which it would apply to cyber incidents, and therefore must be interpreted in favor of coverage."

In ***Merck & Co., Inc., v. ACE American Ins. Co.,*** Super. Ct., Union County, N.J., UNN-L-002682-18, Aug. 2, 2018, Merck also sued property insurers. Merck experienced a network interruption event which led to extensive disruption of its worldwide operations. It did not state an amount, but the Wall Street Journal reported that the "cyberattack cost Merck about $670 million in 2017." Kim Nash, Sara Castellanos and Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs,* **The Wall Street Journal,** June 27, 2018. Merck's property policies covered "all risks of physical loss or damage to property," including any destruction, distortion, or corruption of any computer data, coding program, or software." It did not identify or quote the war exclusion at issue, but simply noted that certain insurers and reinsurers purportedly denied coverage on the ground that the event "was an act of war or terrorism." It sued dozens of insurers and reinsurers (of its captive insurer), so the case has the potential for widespread applicability, if not settled.

It is anticipated that hostile cyber attacks by nations and their agents will increase in the coming years, as will formal attributions. It is likely that these will generate the largest losses. For example, the recent attack on the Marriott hotel chain is believed to have been initiated by China, although no formal attribution has yet been made.

The application of the War Exclusion is addressed at length in Vincent J. Vitkowsky, *War Exclusions and Cyber Threats from States and State-Sponsored Hackers,* May 16, 2017 (private distribution White Paper).

January 8, 2019

Vince Vitkowsky is a partner in Seiger Gfeller Laurie LLP, resident in New York. He focuses on cyber risks, liabilities, insurance, and litigation. Vince assists insurers and reinsurers in product development, including manuscript policies, and in all aspects of coverage evaluation and dispute resolution across many lines of business, including cyber, CGL, and professional liability. He also assists in complex claim evaluations, and if necessary, the defense of insureds in complex matters. Vince can be reached at vvitkowsky@sgllawgroup.com.