GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks and Insurance Coverage Decisions 2015-2019

Vincent J. Vitkowsky

Connecticut New York New Jersey Massachusetts

GFELLER LAURIE LLP
ATTORNEYS AT LAW

Table of Contents

INTRODUCTION

The Internet is the most dynamic engine for economic growth in the world today, and cyberspace is the most dynamic domain. It is also a vortex of risks, including ransomware, cyber extortion, network interruption, data breaches, lost data, lost software, disabled hardware, cryptomining losses, and liability from websites and social media. Deceptive funds transfers and bitcoin theft have also been drawn into the mix.

Before the development of the cyber insurance market, insurance policies either excluded cyber risks, or more commonly, were silent on whether they covered them. Now, many insurance polices cover some — but not all — cyber risks.

The law of cybersecurity, privacy, and related insurance coverage is just beginning to emerge. The last five years have seen an increasing number of disputes concerning what specific risks and losses might be covered under particular lines of business. Prior to this modern era, there were only a few reported decisions, mostly addressing whether lost data, software and hardware, or business interruption losses, were covered under CGL or property policies. The results were mixed. There was a single known case seeking coverage under CGL Coverage B for one of the Sony data breaches, in which the holding of a New York lower court judge, denying coverage, was simply stated at the end of a lengthy hearing transcript.

In the modern era encompassed in this Survey, there have been numerous reported decisions, many carefully reasoned, under CGL, Businessowners, Computer Fraud and Crime, Financial Institution, Cyber, D&O, and even Homeowners policies. Many of those decisions are described herein. They demonstrate that the law of insurance coverage for cyber risks will also be dynamic, addressing many novel, challenging, and knotty issues in the years ahead.

Vince Vitkowsky
New York, NY
January 10, 2020

vvitkowsky@gllawgroup.com
www.gllawgroup.com

Please note that this Survey is for informational purposes only, and is not comprehensive. It does not constitute the rendering of legal advice or opinions on specific facts or matters. The distribution of this Survey to any person does not constitute the establishment of an attorney-client relationship.

CGL AND BUSINESSOWNERS POLICIES

Data Breach and Cyber-Related Privacy Coverage Under CGL and Businessowners Policies

Florida Federal 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., *337 F.Supp.3d 1176 (M.D. Fla. Sept. 28, 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.

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 coverages 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."

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.

Federal 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 federal court in Florida 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.

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

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 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) (see detailed discussion below) 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.

New York Appellate Division Denies Coverage for Data Breach Under Businessowners 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 Businessowner'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 Businessowners 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.

Connecticut Supreme Court Finds No Coverage Under Coverage B for Data Exposure Where There Was No Publication

Recall Total Info. Mgmt., Inc., et al. v. Federal Ins. Co., et al., *317 Conn. 46, 115 A.3d 458 (2015).* The Connecticut Supreme Court decided a case which did not involve a computer hack, but nonetheless was widely-watched in the cyber risk world, drawing amicus curiae briefs from policyholder and insurance industry groups. It involved coverage under CGL and excess policies for an incident in which data tapes containing the personal information of IBM employees fell out of a transport van and were stolen from the side of the road. Following the loss, IBM expended nearly $6M to protect the identity and credit of its employees. The contractors that lost the tapes reimbursed IBM for the costs incurred and brought suit against its Insurers seeking indemnification. The trial court granted summary judgment in favor of the Insurers. On appeal, the Appellate Court agreed with the Insurers' position that coverage was unavailable under either policy, as a matter of law, because the appellants failed to produce any evidence that a third party accessed the information on the tapes or that any IBM employee suffered any damages as result of theft. As such, there was no personal injury, because there was no publication resulting in a violation of a person's right to privacy, as required under the Coverage B "Personal and Advertising Injury" coverage grant. The Connecticut Supreme Court agreed in a *per curiam* opinion which adopted the Appellate Court's opinion.

Third Circuit Finds No Coverage Under Coverage B Where There Was No Publication, *i.e.,* No Dissemination to the Public at Large

OneBeacon America Ins. Co. v. Urban Outfitters, *2015 WL 5333845 (3d Cir. Sept. 15, 2015)*, the Court held that Insurers had no duty to defend or indemnify their Insureds under Coverage B in three putative class actions challenging the collection of customer zip codes. The court applied Pennsylvania law. Two of the three putative class actions alleged that the Insureds collected the data for their own direct marketing and junk mailings, and alleged no disclosure to third parties. The Court found there was no publication, because publication requires dissemination to the public at large. The third putative class action alleged that the Insureds sold the information to third-party vendors, thereby violating California's Song-Beverly Act. The Court found no coverage for that action by virtue of an exclusion for Recording and Distribution of Material or Information in Violation of Law.

Ninth Circuit Finds Coverage B Did Not Apply to ZIP Code Case

Big 5 Sporting Goods Corp. v. Zurich American Insurance Co., et al., *No. 13-56249 (9th Cir. Dec. 7, 2015).* Big 5 sought defense costs for 12 class actions alleging that it had collected, used and sold zip codes in violation of California's Song-Beverly Act. The opinion applied California law, but was not for publication, and hence not binding precedent. The

Court found coverage was barred by virtue of exclusions for personal and advertising injury arising directly or indirectly out of statutory violations. Big 5 had also included claims for common law and California constitutional right to privacy claims. However, the Court said that no such causes of action had ever been recognized in California, and did not exist. The only possible claim is for statutory penalties. Thus the court held that "[a]llowing Big 5's fact pattern to rise to the level of a claim would require an insurance company to insure and defend against non-existent risks."

COMPUTER FRAUD POLICIES

Decisions Finding No Coverage Under Computer Fraud Policies for Deceptive Funds Transfers

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.

Eleventh Circuit Holds There Was 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 than the lower court.

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.

CRIME POLICIES

Decisions Finding No Coverage Under Crime Policies for Deceptive Funds Transfers

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.

Ninth Circuit Finds No Coverage Under a Crime Policy for Social Engineering-induced Deceptive 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 the Insurer 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.

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

***Apache Corp. v. Great American Ins. Co**., 662 Fed.Appx 252, 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. 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."

Decisions Finding Coverage Under Crime Policies for Deceptive Funds Transfers

Eleventh Circuit Finds Coverage for a Deceptive Funds Transfer Under a Crime Policy, Finding a Fraudulent Instruction and Proximate Causation in a Multi-Step Transaction

***Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.,** 944 F.3d 886 (11th Cir. 2019)*. Applying Georgia law, the Eleventh Circuit found coverage for the loss of more than $1.7 million in funds transferred under a sophisticated social engineering scheme. The Insured sought coverage under a Fraudulent Instruction provision covering "[l]oss 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 lower court found coverage on the grounds that the language was ambiguous and should be construed against the Insurer. The Appellate Court did not agree that the language ambiguous, but rather found it *unambiguously* provided coverage.

The well-developed scheme began when the Controller for the Insured received an email purporting to be from Josh Nazarian, a Managing Director of the Insured. It said there was a "secret acquisition" and directed the Controller follow instructions from "attorney Mark Lynch." Five minutes later the Controller received an email from someone purporting to be Lynch, which sent remittance details for a bank in China. As the transfer was initiated, a fraud prevention service at Wells Fargo asked for verification that the transfer was legitimate. The Controller confirmed with Lynch that the Managing Director had approved the transaction. The Controller relayed this to Wells Fargo, which allowed the eire to go through. The next day, the Controller spoke with Nazarian, the Managing Director, who indicated he did not send the original email. Unsuccessful attempts were made to recover the funds.

The Insurer made two arguments. First, it argued there was no "Fraudulent Instruction," which the policy defined as an "electronic or written instruction initially received by [the Insured], which instruction purports to have been issued by an employee, but which in fact was fraudulently issued by someone else without [the Insured's] knowledge or consent." The Insurer argued the initial email only instructed the controller to work with Lynch to wire the funds, but not to wire a specific amount of money to a specific recipient. The Court rejected this interpretation, seeing the initial email as sufficient, and further finding the later email from Lynch providing the transfer details provided the necessary specificity. The Court also held that "nothing in the policy language warrants the assumption that the two emails could not be part of the same fraudulent transaction."

The Insurer's second argument was that the loss did not "result[] directly from" a Fraudulent Instruction. Applying Georgia law, the phrase "resulting directly from" requires proximate causation between a covered event and a loss, and proximate cause is not necessarily the last act or cause, or the nearest act to the injury. The Court held that neither of the two intervening causes, the Controller's communications with Lynch and Wells Fargo's involvement, severed the causal chain from the original email. Although proximate cause is generally a question of fact for the jury, the Court concluded it could decide it as a matter of law because the evidence was clear and led to only one reasonable conclusion.

Indiana Appellate Court Finds Coverage May Exist for Transfers from Hacked Bank Accounts Because of the Insurer's Placing Quotes for a Crime Policy

Metal Pro Roofing, LLC v. Cincinnati Ins. Co., *130 N.E.3d 653 (Ind.App., Aug. 9, 2019, rehearing denied Nov. 7, 2019)*. An intermediate appellate court in Indiana found coverage may exist for the loss of $78,000 transferred from hacked bank accounts under a Crime policy. Although it found that the specific provisions of the policy did not afford coverage, the placing "quotes" referred to computer hackers, so coverage may have been implied. It remanded to the trier of fact the effect of the usual disclaimers, which were contained in the quotes.

The Insured relied on policy provisions for "Forgery or Alteration" and "Inside the Premises – Theft of Money and Securities." The Insurer argued that these did not afford coverage, and the Court agreed. However, the quotes for the relevant endorsement provided that: "While you've taken precautions to protect your money and securities, you run the risk of loss from employees, robbers, burglars, **computer hackers**, and even physical perils such as fire. Give yourself peace of mind with Cincinnati's crime coverage to insure the money and securities you worked so hard to earn." (Emphasis added.) It indicated a premium for the Endorsement of $125.00. The Insured argued for coverage using theories of fraud, fraudulent inducement, and/or estoppel. The Court said that "It would be entirely reasonable for a prospective Insured to read that language [in the placing quote] in that sequence, to mean, 'If you want to be covered for theft by computer hackers, you should buy this endorsement.'"

However, the Court did not conclusively rule on coverage, because the quote had the usual disclaimer: "[T]his is not a policy. For a complete statement of the coverages and exclusions, please see the policy contract." The Court remanded the case, ruling that the trier of fact should decide whether the disclaimer, which it noted appears in fine print at the bottom of the quote, had the effect of neutralizing otherwise misleading language in the quote.

Second Circuit Finds Coverage Under a Crime Policy for Social Engineering-induced Deceptive Funds Transfer When a Computer Code Was 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.

One of the preliminary decisions of the lower court was also significant, allowing discovery into the specific methods of the intrusions used. See the discussion at p**.** 13, below.

Sixth Circuit Finds Coverage under a Crime Policy for Social Engineering-induced Deceptive 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.

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

Medidata Solutions, Inc. v. Federal Ins. Co., *2016 WL 7176978 (S.D.N.Y. March 10, 2016)*. This highly-watched case involved 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 argued 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. In denying summary judgment to both parties, the court in *Medidata* granted leave to conduct expert discovery. The discovery was “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.” Ultimately, the Insured prevailed at the Second Circuit. See the discussion at p. 12**,** above.

FINANCIAL INSTITUTION BONDS

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.

New York Court of Appeals Finds No Coverage Under a Financial Institutions Bond Where Fraudulent Information Was Entered By Authorized Users

Universal Am. Corp v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, *25 N.Y. 3d 675 (2015)*. The highest court in New York applied the language of a financial institution bond to deny coverage for losses that arose from the entry of fraudulent claims into its computer systems by authorized users. Universal American is a health insurer that allows health providers to submit claims directly into its computer system. It allegedly suffered over $18 million in losses for payments of fraudulent claims for services never actually performed.

The bond contained a rider covering "Computer Systems Fraud," which was defined as "Losses resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program into, or (2) change of Electronic Data or Computer Program within the Insured's Proprietary Computer System". However, the bond excluded "losses resulting directly or indirectly from fraudulent instruments which are used as source documentation in the preparation of Electronic Data, or manually keyed into a data terminal." National Union denied coverage. Like the lower courts, the Court of Appeals ruled in its favor. The Court of Appeals concluded that the language of the rider provided coverage for losses incurred through unauthorized access to the computer system, *i.e.,* deceitful and dishonest acts of outside hackers, but not to fraudulent information entered by authorized users.

CYBER POLICIES

Data Breach Claim Under Cyber Policy

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 3055111 (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."

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, an intermediate appellate court, 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.

Tech E&O Claims Under Cyber Policy

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)*. In 2015, 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).

However, 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.

Ultimately, the entire case was voluntarily dismissed.

D & O POLICIES

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, *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.

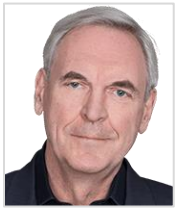
HOMEOWNERS POLICIES

Coverage for Theft of BitCoin Under Homeowners 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., *2018 WL 7252940 (Ohio Com.Pl., filed Sept 25, 2018)*. Plaintiff submitted a claim under his homeowners 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.



Vince Vitkowsky is a partner in 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 endorsements, and in all aspects of coverage evaluation and dispute resolution across many lines of business, including cyber, CGL, property, and professional liability. He also assists in complex claim evaluations, and if necessary, the defense of insureds in complex matters.

vvitkowsky@gllawgroup.com

www.gllawgroup.com