SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

# Cyber and Privacy Coverage Litigation 2015

**Vincent J. Vitkowsky**

New York Connecticut New Jersey

SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

# Cyber and Privacy Coverage Litigation 2015

Vincent J. Vitkowsky

Cyber risks are everywhere. Losses from data breaches, network disruption, technology service failures, media incidents, and computer fraud have become significant risks for all businesses. Insurance products exist to address some of these risks specifically, and insureds have sought coverage under a broader range of policies. In 2015, there were important developments concerning coverage under cyber, tech E&O, crime, and general liability policies. This paper reviews both reported decisions and pending litigation in this rapidly-developing field.

## Cyber Policies Providing Tech E&O Coverage

In ***Travelers Property Casualty Co. of America v. Federal Recovery Services, Inc.,*** 2015 WL 2201797 (D. Utah May 11, 2015), a federal court applying Utah law ruled that Travelers had no duty to defend under its CyberFirst® policy for an insured's refusal to return certain customer information in connection with a merger. The policy included a Technology Errors and Omissions Liability form that provided coverage for "any error, omission, or negligent act." The insureds were Federal Recovery Systems, Inc. and Federal Recovery Acceptance, Inc. (FRA). FRA was a payment processing company that held customer information, including credit card and bank account information, for a chain of fitness centers run by Global Fitness Holdings LLC. Global Fitness entered into an Asset Purchase Agreement pursuant to which it would be purchased by L.A. Fitness, and would transfer all its member accounts data to L.A. Fitness. Global Fitness thus requested that the customer information be transferred back to it. FRA did not transfer all of it, but rather demanded significant compensation. Global Fitness sued FRA for conversion, tortious interference, and breach of contract. The complaint alleged no error, omission, or negligent act. Instead, it alleged that FRA 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.

## Cyber Policies Providing Coverage for Losses from Data Breaches

There are still no reported decisions involving coverage under cyber insurance policies for a data breach incurred through hacking. However, a complaint filed in 2015 involves a scenario that is likely to recur. In ***Columbia Cas. Co. v. Cottage Health Sys.,*** No. 2:15-cv-03432 (C.D. Cal., filed May 7, 2015), Columbia Casualty Company (CNA) issued its NetProtect360 cyber insurance policy to Cottage Health Systems. The policy covered "privacy injury claims." A data breach resulted in release onto the Internet of electronic private healthcare information for approximately 32,500 of Cottage's patients. A class action followed, which was settled for $4.125 million. CNA agreed to fund the settlement subject to a reservation of rights. CNA then filed a declaratory judgment action.in which it denied coverage on two grounds. First, it relied on an Exclusion for "Failure To Follow Minimum Required Practices," based upon Cottage's alleged failure "to continuously implement the procedures and risk controls identified in its application," to "regularly check and maintain security patches on its system," and to "enhance risk controls." Next, it relied on an "Application" condition which stated that the policy shall be null and void if the Application contains any misrepresentation or omission. "Upon information and belief," CNA identified false responses to 10 separate questions on the Application. A separate "Minimum Required Practices" condition provided that the Insured "warrants, as a condition precedent," that Minimum Required Practices would be followed and all risk controls in the Application "and any supplemental information provided by the Insured" would be followed. CNA alleged that the misrepresentations and/or omissions of material fact "were made negligently or with the intent to deceive." Thus, it sought a declaration that it had no obligation to indemnify and that it was entitled to reimbursement of the settlement amount.

Adjudication of these issues was deferred because the court dismissed the complaint without prejudice based on the insurer's failure to follow the mediation procedure set forth in its policy before filing.

## Cyber Policies Providing Media Liability Coverage

Late in 2015, Beazley commenced a declaratory judgment action concerning a Media Tech Liability policy it issued to a broadband communications company. ***Certain Underwriters at Lloyd's, London v. Cox Enterprises, Inc. et al.,*** No. 653849/15 (Sup. Ct., N.Y. Co., filed November 22, 2015) involved claims asserted against Cox by copyright holders. When Cox's customers use its internet service to download copyrighted material such as music and movies, and when the copyright holders or enforcers learn of such instances, the holders notify Cox that there was an infringement. Initially, Cox would forward those notices to the identified customers. Beazley alleges that as the volume of such notices reached the millions, and Cox disagreed with the content of some of the notices, Cox made an intentional business decision not to forward infringement notices and not to block or freeze the alleged infringer's accounts. The copyright holders commenced an underlying action against Cox for contributory and vicarious copyright infringement. In the coverage action, Beazley alleges that coverage does not exist because of Exclusions applying to: (1) intentional violations of

the law; (2) acts, errors, omission or incidents committed or occurring prior to the policy's inception date; and (3) related or continuing acts, errors, omissions, incidents or events where the first one was committed or occurred prior to the policy's retroactive date.

**Crime Policies Providing Computer Fraud Coverage**

The interpretation of crime policies which also insure against computer fraud has arisen in several cases in which employees have been tricked into making improper transfers of funds or assets through "social engineering, *i.e.,* the manipulation of humans into performing acts or divulging confidential information. These are to be distinguished from losses resulting from a direct hack, a virus-induced transfer or an infiltration into a password protected system.

***Apache Corporation v. Great American Ins. Co.,*** 2015 WL 7709584 (S.D. Tex. Aug. 7, 2015) found coverage under a Crime Protection Policy where a fraud was perpetrated through social engineering. Among other coverages, the policy insured against "loss . . . resulting directly from the use of any computer to fraudulently cause a transfer of [money] from inside the premises," which is a common grant in crime policies. Apache received a fraudulent call purporting to be from a vendor requesting a change in the account to which payments due from Apache would be sent. Upon being informed that such a request must be on the vendor's letterhead, the fraudster sent an email with an attachment purporting to be on the vendor's letterhead. An Apache employee called the number on the letterhead to verity the request, the fraudster verified it, and thereafter Apache remitted $2.4 million in payments to the fraudster's account.

These facts presented the question of whether the loss resulted directly from computer fraud. Granting summary judgment, the court held that it did. It applied Texas law holding that the phrase "resulting directly from" is synonymous with a "cause in fact," which in turn means the act in question "was a substantial factor in bringing about the injuries, and without it, the harm would not have occurred." It ruled that the fraudulent email was a substantial factor, and that despite the human involvement following the email, coverage existed. The court rejected the argument that only fraud perpetrated through a direct "hacking" would be covered. This case has been appealed to the Fifth Circuit.

A similar issue is ripe for adjudication in ***Medidata Solutions, Inc. v. Federal Ins. Co.,*** No. 1:15-cv-00907 (S.D.N.Y., filed February 6, 2015). There, a fraudster posing as an executive of Medidata sent an email to an employee in its accounts payable department directing a transfer of funds. The fraudster copied a fictitious attorney. After checking with the "attorney" by email and telephone, the Medidata employee transferred $4.8 million to a bank account in China.

Medidata made a claim under a crime policy providing coverage for losses resulting from Computer Fraud, defined as "fraudulent entry of data into . . . a Computer System"

or a "fraudulent change of data elements . . . of a computer system." Federal denied coverage, Medidata commenced an action, and the parties have cross-moved for summary judgment. Federal argues that there is no coverage because there was no manipulation or unauthorized entry into a computer system, and that there was no involuntary transfer effected by hackers, forgers or impostors. Rather, there was a voluntary transfer effected by authorized users.

Federal relies on an earlier decision from 2015, ***Universal Am. Corp v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*****,** 25 N.Y. 3d 675 (2015). There, 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.

Another pending case involves a claim under a crime policy for a loss incurred through social engineering. In ***BitPay, Inc. v. Massachusetts Bay Ins. Co.,*** No. 1:15-cv-03238 (N.D. Ga., filed September 15, 2015), a Bitcoin payment processor seeks coverage under a commercial crime policy for a portion of the loss of $1.85 million in digital currency occurring after its CFO fell victim to a spear phishing attack. The policy included a Computer Fraud Insuring Agreement, and the language was the same as in the *Apache* case, above. It covered loss of "money" directly resulting from the use of any computer to fraudulently cause a transfer from inside the "premises," and the definition of "money" was amended to include Bitcoin. The complaint alleges that BitPay's CFO, Bryan Krohn, responded to an email from a hacker claiming to be a journalist for the publication yBitcoin, requesting a comment for an article. Krohn was directed to a website where he provided the credentials for his BitPay email account. The hacker then used these credentials to fraudulently cause BitPay to make transfers of Bitcoin. Massachusetts Bay contends that coverage exists only for losses directly resulting from a hack using BitPay's computer system to fraudulently cause a transfer, but here, the loss was caused indirectly by the hack into yBitcoin's computer system. It also asserts that the lost Bitcoins were not covered because they were not physically located in BitPay's offices.

**Cyber and Privacy-Related Claims Under CGL Policies**

Insureds continue to seek coverage for cyber and privacy-related claims under CGL policies. They had some limited success in the past, but the reported decisions in 2015 have not supported such coverage.

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. ***Recall Total Info. Mgmt., Inc., et al. v. Federal Ins. Co., et al.,*** 317 Conn. 46, 115 A.3d 458 (2015), 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.

The other reported decisions in 2015 focused on Coverage B as well. In ***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 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.

The same result was reached by the Ninth Circuit in ***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."

In ***Defender Security Co. v. First Mercury Ins. Co.,*** 2015 WL 569251 (7th Cir. Sept. 29, 2015), a home security systems provider allegedly recorded and stored all incoming and outbound telephone conversations without notice or consent. It was sued in a class action in California state court. In a declaratory action coverage against its insurer, the court held that the mere recording and storage of information did not constitute "Publication." Applying Indiana law, the 7th Circuit affirmed a district court's dismissal of the complaint on the pleadings.

In ***American Economy Ins. Co. v. Aspen Way Enterprises, Inc***, 2015 WL 5680134 (D. Mont. Sept. 25, 2015), an insured allegedly installed spyware on laptops it leased to customers, allowing access to personal data such as keystrokes, screenshots, and images taken from the webcam of individuals in various states of undress. It was sued in a class action alleging violation of the Electronic Communications Privacy Act, 18 U.S.C. 2511 (ECPA), and common law invasion of privacy. It was also sued by the State of Washington. The insured sought a defense and indemnity under Coverage B. Applying Montana law, the district court found that the action by the state did not allege facts that would constitute publication, but the consumer class action did. Yet because of the claimed ECPA violation, the exclusion for Recording and Distribution of Material In Violation of Law applied. The court granted summary judgment in favor of the insurer.

**Another Case of Interest**

***Merrick Bank Corp. v. Chartis Specialty Ins. Co.,*** No. 12-cv-7315 (RJS) (S.D.N.Y. March 20, 2015). This case involved the interpretation of a specialized "Uncollectible Chargeback" policy. The policy covered the risk that Merrick Bank was exposed to as a clearing bank for merchants selling goods or services through credit and debit card transactions. In that capacity, Merrick is required to refund the issuing banks for chargebacks of transactions that are disputed by customers, and faces the risk of being unable to collect the amounts refunded by it from the merchants. The policy required indemnity for losses in excess of certain amounts, tied to the collateral in any applicable merchant reserve account. The operation of the policy depended upon the construction and interrelationship of several provisions. On cross-motions for summary judgment, the court found the policy to be ambiguous. It applied the rule that *contra proferentem* does not operate under New York law where the insured is a sophisticated party, represented by a broker, and where the parties actually negotiated the policy. *Contra proferentem* is also inapplicable where there is extrinsic evidence from which inferences of intent can be drawn. After conducting a detailed examination of the available extrinsic evidence, the court concluded that a jury could reasonably draw multiple inferences, and hence summary judgment was not appropriate. Of particular interest,

the broker had given deposition testimony that supported the insurer's interpretation. Nonetheless, the court declined to conclusively impute that interpretation to its principal, the bank. In addition, the court found that the Other Insurance provision did clearly and unambiguously require that the liability of Chartis, if any, would be in excess of any amounts recoverable against third parties. However, it found that the actual amounts recoverable were in dispute and also required resolution by the jury.

## Conclusion

The Internet is the most dynamic engine for economic growth in the world today, and cyberspace is the most dynamic domain. The law of cybersecurity, privacy, and related insurance coverage is just beginning to emerge. It too will be dynamic, presenting many novel, challenging, and knotty issues in the years ahead.

December 2015

*Vince Vitkowsky is a partner in Seiger Gfeller Laurie LLP, resident in New York. He represents insurers in coverage and reinsurance matters across many lines of business, including cyber insurance. 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.*