Under Attack – The Deluge of Cyber Attacks and Industry Response

Kevin T. Coughlin, Esq.
Steven D. Cantarutti, Esq.
Jonathan A. Messier, Esq.

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NJ 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 28TH FL.
NEW YORK, NY 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

TABLE OF CONTENTS

Page

I. Introduction

As the headlines reveal on an almost daily basis, cyber attacks and other data breaches have significantly increased in the United States and around the world the last two years. According to one report, 2013 was the year of the "mega breach," which included: a 91% increase in targeted attacks; a 62% increase in the number of data breaches; and over 552 million identities exposed from data breaches.[1] In fact, the United States accounted for 39% of the total number of cyber attacks in 2013 across the globe, an astounding number when you think that the United Kingdom came in a distant second at 5%, followed by India at 3%.[2]

Despite efforts by businesses and governments in the United States to increase their efforts to prevent cyber attacks, the trend has continued through 2014.[3] Just in the last few weeks, cyber attacks were reported against Home Depot (56M credit and debit card records potentially exposed), UPS (100,000 transaction records exposed from 51 stores), Apple (photos belonging to over 100 celebrities and models were stolen from its cloud system), and Sony (PlayStation network was shut down for several hours due to denial of service attacks). Perhaps the most alarming trend is the healthcare industry, where cyber attacks have reportedly increased 600% in the past 10 months.[4] Litigation regarding cyber attacks is also growing.

With cyber attacks and other data breaches on the rise throughout the United States, it is not surprising that coverage disputes involving cyber-related claims have also heated up. Insureds seeking recovery from their insurers for first-party losses and third-party liabilities have sought coverage under third-party commercial general liability ("CGL") insurance policies, while insurers have resisted such claims taking the view that cyber-related claims were never intended to be covered under such policies. Due to these conflicts, courts across the United States have increasingly weighed in on resolving these coverage disputes.

While cyber specific claims-made policies have been available for years, the limits for these policies have been modest and the premium costs high. This has acted as a disincentive for companies to secure cyber risk policies.

---

[1] *See* "Highlights from the 2014 Internet Security Report," by Semantec Corp, available at: http://www.symantec.com/security_response/publications/threatreport.jsp

[2] *See* "2013 Cyber Attacks Statistics" by Hackmageddon.com, available at: http://hackmageddon.com/?s=top+10+countries+2013

[3] According to a report cited by Business Insurance, the number of data breaches through July 2014 is 411, an increase of 20.5% during the same period last year. *See* "Reported data breaches running 20.5% higher than in 2013: Report," by Business Insurance, available at http://www.businessinsurance.com.

[4] *See* "Hackers are Homing in on Hospitals," by MIT Technology Review, available at: http://www.technologyreview.com/news/530411/hackers-are-homing-in-on-hospitals/.

The paper will address the impact of cyber attacks and other cyber-related claims on insurers and insureds and how courts have addressed these complex issues. More specifically, this paper will include a survey of significant decisions made by courts within the last few years that addresses whether CGL policies and other types of first and third-party policies provide coverage for these type of claims. As explained below, while the results have been mixed for cyber-related data breach claims, one state court has held that there is no coverage under CGL policies for claims involving cyber attacks. Finally, this paper will address the insurance industry's response to the rise in cyber-related claims and the growing market of "cyber-risk" insurance products.

II. Overview of Cyber Attacks

A. What are Cyber Attacks?

Cyber attacks have become a distinct class of risk increasingly faced by insureds. As the "internet of things" expands, the probability increases that the insureds marketing internet-ready products, including the hardware or software components of those products, will experience a cyber attack. At its core, a cyber attack involves the theft and potential release of information to unintended parties due to the malicious acts of an individual or entity doing the hacking.

A distinct part of cyber attacks is a data breach. According to the Mirriam-Webster Dictionary, "breach" includes "a gap (as in a wall) made by battering." But the definition also includes "a failure to do what is required by a law, an agreement or a duty; failure to act in a required or promised way." These definitions are both appropriate, given that insureds generally bear substantial first party losses *and* damages for third-party losses in connection with a data security breach due to a cyber attack. The risks to a business of cyber attacks include civil liability, criminal liability, damage to real or intangible property, interruption of business, and loss of reputation. That disparate risks arise from a single attack is not surprising. What is surprising is the range of potential threats—foreign governments, political provocateurs, non-governmental criminal syndicates, aggrieved employees and even bored teenagers—and the lack of a structured manner in which to reduce the risk of cyber attacks, despite the best efforts and intentions of insureds.

Cyber attacks may arise due to flawed data security architecture, flawed implementation of data security protocols, carelessness of employees, or a combination of those factors. The causes of cyber attacks are varied, decentralized, difficult to quantify, and evolving. Relative uniformity in data security architecture enables key features of a cyber attack to be applied to the next target with ease and rapidity. Indeed, a recent study found that 94% of all data security breaches involve nine basic patterns of attack.[5] Further compounding this quandary is the

[5] *See* Verizon Enterprise Solutions, 2014 Data Breach Investigations Report 13 (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

tension faced by data security professionals in making networks secure for employees and customers.

By way of example, only 1% of point-of-sale cyber attacks—which are attacks at the point in the sale of goods or services where money is provided by the customer to the merchant—are discovered by the target through its own efforts.[6] Notably, it is generally third parties—not the targets of cyber criminals—that discover cyber attacks. An insured is most likely to learn of a cyber attack from law enforcement or exterior fraud detection services.[7] Law enforcement and fraud detection services generally discover cyber attacks only *after* cyber criminals begin exploiting the stolen data.[8] Discovery by those sources usually takes place within weeks or months after the attack.[9]

B. High-Profile Cyber Attacks

As stated in the introduction, large and sophisticated companies responsible for securing personal and financial information of thousands, if not millions, of customers have been particularly exposed to cyber attacks. The following is a summary of the most significant cases involving cyber attacks within the last few years:

- Sony: On or about April 17 and 19, 2011, one or more computer "hackers" launched criminal cyber attacks against Sony's PlayStation Network and Qriocity services (collectively, "PSN") and the Sony Online Entertainment Network ("SOE Network") (collectively with PSN, the "Networks"). The computer hackers allegedly obtained illegal access to and stole personal identification and financial information belonging to over 100 million customers of the Networks. The stolen personal information included customer names, home addresses, email addresses, user credentials, and credit/debit card information. Sony was forced to shut down the Networks for several weeks. Sony also faced numerous class action lawsuits from its customers, which claims are also the subject of a declaratory judgment action pending in New York state court, as explained below.

- Adobe Systems: Around the same time as the Sony breach, software giant Adobe Systems suffered an attack on its network. The attackers stole source code for Adobe Systems' popular Photoshop, Acrobat, ColdFusion, and ColdFusion Builder software and customer information for nearly 38 million customers. The customer information included debit/credit card information, encrypted customer login credentials, and unencrypted answers to security questions. Cyber criminals set up various phishing scams following the attack in order to match the encrypted

[6] *Id*. at 18.
[7] *Id*.
[8] *Id*.
[9] *Id*.

customer login credentials with the unencrypted answers to security questions. Adobe was sued in a class action lawsuit alleging, among other things, failure to implement reasonable security practices.

- Target: On or about November 30, 2013, cyber criminals allegedly "hacked" into the computer system of a vendor of Target, thereby obtaining access to Target's secured computer networks. From there, criminals were able to install malware at point-of-sale terminals in each of Target's 1,797 stores in order to skim customer credit/debit card information. Ironically, Target had a $1,600,000 computer system to detect the attack and automatically delete the malware. Nonetheless, Target had disabled certain functions of the computer system, thereby enabling the cyber criminals to steal 40 million credit/debit card numbers and 70 million customer addresses. More than 100 lawsuits have been filed against Target by aggrieved customers and banks.

- Michaels: During January 2014, cyber criminals penetrated the computer systems of Michaels' stores and stole up to 2.6 million records containing credit/debit card numbers belonging to customers. The criminals installed malicious software at point-of-sale terminals at certain Michaels and Aaron Brothers stores. Michaels has been sued in a class action lawsuit as a result of the breach.

- Home Depot: On September 8, 2014, Home Depot reported that it suffered a cyber attack using the same malware as the Target attack. The attack occurred as Home Depot was rolling-out a data security system to combat this type of attack. The attack targeted point-of-sale terminals—in particular, self-checkout lanes, and skimmed customer credit/debit card numbers. Up to 56 million credit/debit cards were potentially exposed. In the weeks following the attack, networks of criminals telephoned banks' customer service lines with enough data points on the Home Depot customers to change the pin numbers on debit card, thereby enabling the criminals to drain balances on the card. Home Depot is the subject of a multi-state investigation by state attorneys general as well as class action and individual civil lawsuits.

C. Estimated Costs of Cyber Attacks

The Center for Strategic and International Studies ("CSII") has attempted to quantify some costs associated with cyber attacks. CSII estimated that the cost of two subsets of attacks, cyber espionage and cybercrime, to targets in the United States is in the range of 0.5% to 1% of

national income.[10] The dollar amounts could range from $70 to $140 billion per year.[11] On a global scale, the dollar figures could reach $400 billion per year.[12] These figures do not account for the loss of a business's competitiveness due to the theft of its intellectual property, the displacement of workers due to unlawful technology transfers, and lost economic output felt many years after a cyber attack.[13] Thus, losses can be quite substantial on a macro level.

Insureds targeted in cyber attacks may bear losses in the form of costs to: retain crisis-mitigation public relations firms; investigate, monitor, and repair computer networks; notify the appropriate governmental authorities of a breach; and comply with governmental investigations. Insureds may face present and future business losses due to the exposure of trade secrets to unauthorized competitors or the loss or corruption of business data. Insureds also commonly face third-party liabilities from lawsuits filed from aggrieved customers who have had their unencrypted personal information exposed or from payment processors who bear losses as a result of fraudulent transactions or reissuing credit and debit cards due to an attack.

A potential area of exposure for insureds is liability in violating state breach-notification laws after suffering a cyber attack or data breach. A patchwork of state laws now exist requiring varying degrees of compulsory notification by businesses affected by a cyber attack. Only four states lack breach-notification laws.[14] In addition, the United States Securities and Exchange Commission requires publicly-traded companies to disclose "material information" concerning cyber attacks and other data security breaches to shareholders.

The costs to comply with breach-notification laws are growing. The patchwork of laws requires insureds operating in multiple states to determine which laws must be complied with and which amount of information to supply. In addition, the laws are beginning to offer remedies to individuals whose unencrypted personal information has been exposed in a cyber attack. For example, businesses operating in California that offer customers credit monitoring services in response to a cyber attack must notify their California customers that credit monitoring services will be provided for at least twelve months at no cost to the California customers.[15] This "notification" requirement essentially provides a substantive remedy for aggrieved California customers. It will be interesting to see which additional remedies are added to breach-notification laws and whether a national standard is developed in response.

---

[10] *See* McAfee & Center for Strategic and International Studies, The Economic Impact of Cyber Crime and Cyber Espionage 16 (July 2013), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.
[11] *Id*.
[12] *Id*.
[13] *Id*.
[14] Guam, Puerto Rico, the Virgin Islands, and the District of Columbia also have breach-notification laws.
[15] *See* Cal. Civil Code 1798.82(d) (2) (G).

III. Survey of Recent Case Law

Given the prevalence of cyber attacks and other data breaches in the last few years, it is not surprising that coverage disputes between insureds and their insurers have also intensified for these types of claims. Notwithstanding the fact that cyber risk policies have existed since the late 1990's, insureds who have not purchased such coverage or face claims that exceed their cyber coverage often look to "traditional" first and third-party insurance policies to pay these claims. Insurers, on the other hand, have vigorously denied that cyber attack claims are covered under traditional policies.

Among the most heated battles are attempts by insureds to secure coverage under CGL policies. These policies have been a staple in insurance coverage programs in companies (large and small) for decades because they provide a broad number of coverage types with respect to both defense and indemnity costs. These often include the following:

- Coverage A: provides protection against "bodily injury" or "property damage". "Bodily injury" includes sickness or disease or death, while "property damage" includes physical injury to tangible property, including loss of use of that property, or loss of use of tangible that is not physically injured.

- Coverage B: provides protection against "personal and advertising injury liability". This coverage part includes several enumerated intentional torts, including false arrest, detention, or imprisonment, malicious prosecution, invasion of the right of private occupancy, slander, liable, oral or written publication, in any manner, that violates a person's right to privacy, use of another's advertising idea, and intellectual property infringement.

Of the coverage afforded in CGL policies, insureds often argue that cyber attacks or data breaches are covered as "property damage" (Coverage A) or as an oral or written publication in violation of privacy rights (Coverage B). With respect to "property damage," coverage often depends upon whether electronic data is considered tangible property within the meaning of that defined term. Most, if not all, of the CGL policies today contain definitions or exclusions that exclude "electronic data" as being tangible property. As for the oral or written publication offense, courts have focused upon whether (i) a "publication" has been alleged or occurred, (ii) who made the publication, and (iii) whether privacy rights have been violated. In addition to examining the provisions in the insuring grants, coverage is also dependent upon whether any exclusions may apply, such as the exclusion in Coverage B that bars coverage for the violation of any statute that prohibits the sending, transmitting, communicating, or distribution of material or information.

This next section provides a survey of recent cases that have decided cyber-related claims under CGL policies as well as other traditional policies, such as first-party property insurance or crime policies. As explained below, courts have made significant rulings in this relatively "new" and emerging area of insurance law, which has been favorable for both insurers and insureds. Although some of the cases we include arise from the disclosure of confidential information by the insureds themselves, not due to hackers or other third-parties, we have included them in our discussion as they may be potentially applicable for claims arising from cyber attacks.

A. Comprehensive General Liability Policies

i. Recall and Portal: When is Loss of Data Considered a "Publication"?

Two recent courts, reaching different results, addressed the issue of when a loss of data becomes a "publication" for the purpose of triggering the "oral or written publication" offense. Both courts examined the meaning of the undefined term "publication" and whether access to the confidential information by a third-party is necessary in order to trigger coverage.

In *Recall Total Information Management, Inc. v. Federal Insurance Company*, 83 A.3d 664 (Conn. App. Ct. 2014), the Appellate Court of Connecticut held that an insurer did not have a duty to indemnify an additional insured for a claim involving the loss of 130 IBM computer tapes by its subcontractor. The additional insured, Recall Total Information Management, Inc. ("Retail"), entered into an agreement with IBM to transport and store various electronic media belong to IBM. *Id.* at 453. Recall, in turn, entered into a subcontract with Ex Log to provide transportation services for the electronic media. Pursuant to the subcontract agreement, Ex Log purchased primary and umbrella CGL policies naming Recall as an additional insured. On February 23, 2007, Ex Log was transporting the IBM tapes from a facility in New York to another location when the cart containing the tapes "fell out of the back of a van near a highway exit ramp." *Id.* The tapes, which contained employment-related data for approximately 500,000 past and present IBM employees, were removed from the roadside by an unknown person and were never recovered.[16] *Id.* at 454.

Recall agreed to pay IBM more than $6 million for costs that IBM had incurred to prevent harm arising from the dissemination of the information.[17] Thereafter, Recall sought reimbursement from Ex Log, which resulted in a settlement in which Ex Log agreed to assign its rights to Recall to collect against the CGL primary and umbrella policies. In the declaratory judgment action filed by Recall and Ex Log (collectively, "Plaintiffs"), the trial court granted summary judgment to the insurers, concluding, *inter alia*, that there was no "property damage" because the "data loss constituted intangible property, which was expressly excluded from

[16] The data included social security numbers, birthdates, and contact information. *Id.* at 454.

[17] This included notifying all of the potential affected employees, establishing a call center to answer inquiries about the lost data, and providing employees with one year of credit monitoring services to protect against identity theft. *Id.*

coverage." *Id.* at 455. As for the "personal injury" provision, the trial court held that there was no evidence that anyone had accessed tapes that would have violated the right to privacy.[18]

In affirming the decision, the Appellate Court rejected Plaintiffs' arguments that the mere loss of the tapes constituted a "publication" or that it may have been "published" to the thief.[19] *Id.* at 462. The court noted that Plaintiffs had "failed to cite any evidence that the information was published and thereby failed to take their allegation beyond the realm of speculation." *Id.* In particular, the Appellate Court found that the "complaint and affidavits [were] entirely devoid of facts suggesting that the personal information actually was accessed . . ." *Id.* The Appellate Court also held that regardless of the precise definition of the term "publication," access to the information is "a necessary prerequisite" in order to find "publication". Given that Plaintiffs had presented no evidence that the tapes were accessed by anyone, the Appellate Court held that they failed to meet their burden that a publication had occurred.[20] *Id.* at 463.

The Federal District Court of the Eastern District of Virginia in *Travelers Indem. Co. of Amer. v. Portal Healthcare Solutions, LLC*, 2014 U.S. Dist. LEXIS 110987 (E.D. Va. Aug. 7, 2014), on the other hand, held that a "publication" had occurred even though there was no evidence that anyone (other than the patients themselves) had accessed their confidential medical records. Portal Healthcare Solutions, LLC ("Portal"), a business specializing in the electronic safekeeping of medical records, had posted the confidential medical records of patients on the internet. Some of the patients noticed their records after performing a "Google" search of their names, which prompted a class-action lawsuit against Portal. The CGL policies issued to Portal contained endorsements that defined "Personal Injury" to include: "Oral, written or electronic publication of material that . . . gives unreasonable publicity to a person's private life" (2012 CGL policy); or "Oral or written publication, including publication by electronic means, that . . . [d]iscloses information about a person's private life" (2013 CGL policy).

The district court held that Travelers had a duty to defend Portal's in the class action lawsuits because exposing confidential medical information online was conduct that fell within the activity stated in the personal injury endorsement. *Id.* at *9-17. More specifically, the court found that placing this information online caused "unreasonable publicity" or "disclos[ed] information about" a person's private life. The district court rejected Travelers' arguments that Portal did not intentionally expose the records to the public or that was no allegation that a third-

[18] "Personal injury" was defined as "injury, other than bodily injury, property damage or advertising injury, caused by an offense of . . . electronic, oral, written or other *publication* of material that . . . violates a person's right to privacy." *Id.* at 462 (emphasis in original).

[19] Plaintiffs did not challenge the trial court's decision with respect to whether the loss of computer tapes resulted in covered "property damage".

[20] The Appellate Court further held that even though IBM had a duty to notify its affected employees about the lost tapes under certain statutes, this alone did not trigger the personal injury provision either. As the Appellate Court pointed out, these statutes did not address compensation due to any identity theft, but rather merely required notification to protect an affected person against potential harm. *Id.* Plaintiffs have appealed the ruling, to which the Connecticut Supreme Court granted certification on March 5, 2014. *See Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 86 A.3d 469 (2014).

party had viewed the information. The district court reasoned that the plain definition of the term "publication" did not depend upon the publisher's intent or whether a third-party has access to the information. The district court explained that a "publication" occurs when the information is "placed before the public" and not when "a member of the public reads the information placed before it." *Id.* The district court also distinguished the *Recall* case, because the information there was allegedly given only to a single thief and it was not posted on the internet.[21]

ii. Sony: Must the Insured Affirmatively Act to Cause the Publication in order to Trigger the Oral or Written Publication Offense?

A New York state trial court in *Zurich American Insurance Company v. Sony Corp. of America*, Index No. 651982/2011 (N.Y. Sup. Ct. N.Y. Cnty. Feb. 21, 2014), also made a significant ruling with respect to the "publication" issue in the context of cyber attack claims, by focusing on whether the "oral or written publication" must be made by the insured in order to trigger coverage. In *Sony*, certain Sony defendants, Sony Computer Entertainment America LLC ("SCEA") and Sony Corporation of America ("SCA") (collectively, "Sony"), moved for partial summary judgment against their respective primary general liability insurers -- Zurich American Insurance Company ("Zurich")[22] and Mitsui Sumitomo Insurance Company of America ("Mitsui") – to pay for defense costs incurred in numerous pending underlying class action lawsuits. Zurich and Mitsui, in turn, cross-moved on the same issues. As stated above, the lawsuits arise from cyber attacks that were launched by computer hacks against Sony's Networks in or about April 2011, which exposed confidential personal and financial information belonging to over 100 million of Sony's customers and users.

In their motion, Sony argued that under Coverage B (Personal and Advertising Injury), the primary policies issued by Zurich and Mitsui alleged a potentially covered offense of an "oral or written publication, in any manner, of material that violates a person's right of privacy" (the "Oral or Written Publication Offense"). In their oppositions and cross-motions, Zurich and Mitsui argued that their respective primary policies did not afford coverage under the Oral or Written Publication Offense. Zurich also argued that coverage was barred against SCEA under the "Insureds In Media And Internet Type Businesses" exclusion (the "Internet Business Exclusion"), which excludes certain Coverage B offenses, including the Oral or Written Publication Offense, committed by an insured whose business is "[a]n Internet search, access, content or service provider."

At the conclusion of the arguments for the motions, the trial court issued its decision on the record by first ruling that the Internet Business Exclusion did not apply against SCEA because its business is not entirely based on internet-related activities. Although Zurich argued that courts in other jurisdictions have held that this exclusion can apply as long as the

[21] The district court also disagreed with Travelers' argument that there was no "publicity" or "disclosure" of information, as the conduct of posting information online fell within the plain meaning of these terms.
[22] Zurich is represented by Coughlin Duffy, LLP.

enumerated activity is a "primary, essential, chief or principal" business for the insured, the trial court disagreed with this argument because there was no qualifying language in the exclusion.

With respect to the "publication" issue, the trial court acknowledged that this is a case of first impression involving cyber attack claims. The trial court first focused on meaning of the undefined term "publication" within the Oral or Written Publication Offense and concluded, as in *Portal*, that a "publication" can occur as long as the information becomes potentially exposed for the public to view. As the trial court explained:

> Because, I look at it as a Pandora's box. Once it is opened it doesn't matter who does what with it. It is out there. It is out there in the world, that information. And whether or not it's actually used later on to get any benefit by the hackers, that in my mind is not the issue. The issue is that it was in their vault. Let's just say to visualize this, the information was in Sony's vault. Somebody opened it up. It is now, this comes out of the vault. But, whether or not it's actually used that is something separate, that's separate. On the one hand it is locked down and sealed. But now you have opened it up. You cannot ignore the fact that it's opened for everyone to look at.

Accordingly, the trial court rejected Zurich's argument that there was no publication because the information was stolen by the computer hackers. Rather, the fact that the information escaped was sufficient to be deemed a "publication" from the trial court's view. However, the trial agreed with Zurich that the term "in any manner" means the medium in which the information is published and does not mean, as Sony had argued, that it could amount to a "publication" made by anyone, including third-parties.

Most significantly, the trial court ultimately ruled in favor of Zurich and Mitsui by requiring an affirmative act of publication by the insured in order to trigger coverage under the offense. The trial court found that the underlying class actions were the result of criminal computer hackers obtaining illegal access to the confidential information and Sony's liability was based upon its failure to maintain proper security and to keep that information safe. When the information was accessed and stolen by the hackers, there was a "publication". However, the "publication" offense can only be read to require that the insured act to cause the publication, and cannot be expanded (as Sony argued) to allegations of "negligence" leading to a publication caused by a third party. As the trial court explained:

> I am not convinced that that [*sic*] is oral or written publication in any manner done by Sony. That is an oral or written publication that was perpetrated by the hackers. In any manner, as Zurich's counsel pointed out, means oral or written publication in any manner. It is the medium. It is the kind of way it is being publicized. It's either by fax, it is either by e-mail, either by so forth. But, it doesn't define who actually sends that kind of publication. And in this

> case it is without doubt in my mind, my finding is the hackers did this. The 3rd party hackers took it. They breached the security. They have gotten through all of the security levels and they were able to get access to this. That is not the same as saying Sony did this. But, when I read [the Oral or Written Publication Offense, it] can only be in my mind read that it requires the policyholder to perpetrate or commit the act. It does not expand. It cannot be expanded to include 3rd party acts.

Thus, the Court concluded that Sony was not entitled to coverage for the class action lawsuits under the primary policies issued by Zurich and Mitsui and granted their cross-motions.[23] The trial court's decision marked the first of its kind by any court in the United States that addresses whether CGL policies may be liable to cover claims involving cyber attacks, and sends a loud message to insureds that cyber attacks caused by computer hackers are not covered by these policies.

iii. Coinstar and Corcino: Do Statutory Violations Trigger Coverage under the "Publication" Offense?

Following the *Sony* decision, the Federal District Court for the Western District Court of Washington in *National Union Fire Insurance Company of Pittsburgh, PA v. Coinstar, Inc.*, 2014 U.S. Dist. LEXIS 109338 (W.D. Wash. Aug. 7., 2014), also held that a CGL insurer (National Union) had no duty to defend its insured in two class action lawsuits alleging the unlawful collection and distribution of personal information in violation of statutory laws in Michigan and California. The issues before the district court in this case focused on whether (i) an exclusion barred coverage because the class actions were solely based upon statutory violations, and (ii) liability arising from the statutes themselves required the violation of privacy rights, so as to trigger coverage under the "Oral or Written Publication Offense.

In *Coinstar*, National Union issued two one-year CGL policies in effect between September 1, 2009 and September 1, 2011 and listed Redbox Automated Retail, LLC ("Redbox") as an insured. Redbox operated self-service kiosks in which customers were able to rent movies on DVDs and Blu-ray discs and according to the two class action lawsuits, had allegedly violated certain statutes by impermissibly collecting information from customers or using and sharing that information without consent from its customers. *Id.* at *2-3. The CGL policies at issue contained the Oral or Written Publication Offense and Exclusion (p), entitled "Violation of Statutes in Connection with Sending, Transmitting or Communicating Any Material Or Information," which barred coverage for violating any statute that "addresses or applies to the sending, transmitting, or communicating of any material or information, by any means whatsoever." *Id.* at *4-5.

[23] Sony has appealed the trial court's decision to the New York Appellate Division, First Department, which appeal is scheduled to be argued during the December 2014 Term.

The district court held that in the first class action lawsuit, Exclusion (p), by its terms, applied because that action alleged liability based upon violation of Michigan's Video Rental Privacy Act ("VRPA").[24] *Id.* at *10-15. In other words, because the alleged violation under this statute prohibited an entity from sending customer information to third parties, this type of conduct fell within the scope activities encompassed in the exclusion.[25] *Id.*

As for the second class action, the district court found that although Exclusion (p) did not apply, there was no coverage under the Oral or Written Publication Offense. *Id.* at *15-18. The district court pointed that the plaintiffs in the second class action lawsuit alleged violation under California's Song Beverly Credit Card Act, Cal. Civ. Code § 1747.08 ("Song Beverly Act"), which prohibits entities that accept credits card for business transactions from requesting or requiring the customer to write or provide any personal identification information on a credit card transaction form. Thus, the liability in this case was not based upon any "oral or written publication," as required under the policy. The district court acknowledged that the complaint also contained allegations that Redbox had used Zip codes collected for marketing purposes, had shared its personal information databases with outside entities, and profited by sending marketing information to its customers based upon the information collected. However, the district court concluded that those allegations were not relevant to establish liability under the Beverly Sony Act, which "rests solely on allegation that Redbox wrongfully requested or collected personal information from its customers." *Id.* at *17.

The *Coinstar* case demonstrates that in situations where the alleged statutory violation is based the sending, transmitting, or communication of information, Exclusion (p), or an exclusion containing similar language, may preclude coverage. Even where Exclusion (p) may not apply, the Oral or Written Publication may not be triggered where the basis for liability under the statute does not expressly involve a "publication" of any information.

In *Hartford Casualty Insurance Company v. Corcino & Associates*, 2013 U.S. Dist. LEXIS 152836 (C.D. Cal. Oct. 7, 2013), a California state trial court also addressed whether an exclusion barred coverage in lawsuits alleging unauthorized online disclosures of medical records. In this case, Stanford Hospital and Clinics ("Stanford") and Corcino & Associates ("Corino") had been sued in two state court actions for allegedly violating plaintiffs' privacy rights for posting confidential medical information on a public website.[26] The plaintiffs' causes

[24] The VRPA, *inter alia.*, prohibits entities engaged in the business of selling at retail, renting, or lending video recordings from "disclos[ing] to any other person, other than the customer, a record or information concerning the purchase, lease, rental or borrowing of those materials by a customer that indicates the identity of the customer." *Id.* at *4.

[25] The district court's holding followed a similar decision made earlier in the year in the same case involving another class action lawsuit against Redbox, which granted National Union's summary judgment motion, in part, that it had no duty to defend the class action based upon the application of Exclusion (p).

[26] The plaintiffs alleged that Stanford supplied the information to Corcino, who, in turn, gave it to a job applicant to perform certain tasks with the data as part of a "test for employment suitability." *Id.* at *3-4. The plaintiffs further alleged that after the job applicant posted the information on a public website as part of the test, it remained there for almost a year until one of the plaintiffs discovered it. *Id.*

of action included violations of their constitutional right of privacy, common law privacy rights, violation of California Civil Code § 56.36, *et seq.* ("Confidentiality of Medical Information Act" or "CMIA"), and California Welfare & Institutions Code § 5330 *et seq.* ("Lanterman Petris Act" or "LPS"). *Id.* at *5.

The CGL policy issued to Corcino contained the "personal and advertising injury" insuring clause, which covered "electronic publication of material that violates a person's right of privacy." The policy also contained an exclusion that barred coverage for personal and advertising injury "arising out of the violation of a person's right of privacy created by any state or federal law," but also contained an exception for "liability for damages that the insured would have in absence of such state or federal act." *Id.* at *6. The insurer (Hartford) argued there was no coverage for the "statutory relief" sought in the underlying lawsuits. Stanford moved to dismiss the declaratory complaint filed by Hartford, arguing that the exclusion should not apply because the right to medical privacy was not created by the statute, but rather is an existing constitutional and common law right.

The federal court agreed with Stanford, holding that "the Exclusion applies if, and only if, a claim arises out of the invasion of a private right that is created by statute." *Id.* at *11. The federal district court noted that since at least 1931, California has recognized both a constitutional privacy right and common law tort for violations of the right to privacy. *Id.* at *12. The district court also explained that the legislative history of the LPS and CMIA revealed that these statutes did not intend to "create new rights, but rather to codify existing rights and create effective remedies that would encourage affected individuals to enforce them." *Id*. at *13. Accordingly, because the LPS and CMIA did not create new rights, the district court concluded that they fell within the exception of the exclusion. *Id.*

B. First-Party Property Insurance

Although the coverage terms in first-party property insurance are often even more specialized or limited than those in CGL policies, this doesn't stop insureds seeking coverage for cyber attacks or data breaches. As we see in the next two cases, the court strictly interpreted the terms of the policy and denied coverage in each case.

In *Metro Brokers, Inc. v. Transportation Insurance Co.*, 2013 U.S. Dist. LEXIS 184638, (N.D. Ga. Nov. 21, 2013), the issue before the Federal District Court for the Northern District of Georgia was whether the fraudulent electronic transfer of funds fell within the scope of coverage provided in a business policy that included first-party property coverage. In *Metro*, a thief had logged into the insured's (Metro) online client escrow account, using a key logger virus to learn the login credentials, and had transferred the funds to several other banks throughout the United States. *Id.* at *2. The business policy at issue contained an endorsement that covered "loss resulting directly from 'forgery' or alteration of, on, or in any check, draft, promissory note, bill of exchange, or similar written promise . . . ." The business policy also excluded coverage for

any "malicious code" and "system penetration." The district court rejected Metro's claim for two reasons.

First, the district court found that it was "clear" the fraudulent electronic transfers did not involve "a check, draft, promissory note, [or] bill of exchange." *Id.* at *13-15. Accordingly, the district court focused on whether the electronic transfers constituted "a similar written promise, order, or direction to pay a sum certain," which it determined fell into the same class as negotiable instruments. Upon comparing the meaning of "negotiable instruments" and "electronic fund transfers" under federal and state statutory law, the district court concluded that the latter was not in the same class as a check, draft, promissory note or bill of exchange. *Id.* at *16. The district court also agreed with the insurer that there were no paper copy of the actual transfer requests nor any written requests, but rather they were "triggered by the click of a button and a series of electronically transmitted codes." *Id.* at *17.

Even though the district court found no coverage within the insuring grant, it went on to hold that claims at issue were also barred by the "malicious code" or "system penetration" exclusions. The insured argued that the exclusions should not apply as the virus was not the proximate cause of the loss because a person had to search and analyze the stolen information and use that information in order to gain access to the online banking system. The district court found, however, that despite the human capital involved in the theft, the exclusions contained "anti-concurrent" language, which excluded any loss "regardless of any other cause or event that contributes concurrently or in any sequence to the loss." *Id.* at *20-21. The district court, therefore, found that the virus' role in contributing to the loss was not too remote to fall outside the exclusions.

In *Nationwide Insurance Co. v. Hentz*, 2012 U.S. Dist. LEXIS 29181 (S.D. Ill. Mar. 6, 2012), the Federal District Court for the Southern District of Illinois examined whether a CD-ROM that was stolen from the car of an insured accountant could be covered as "property damage." The CD-ROM contained the names and personal information of approximately 30,000 participants and beneficiaries of a pension fund. The pension fund spent approximately $200,000 in notifying the affected individuals and had contracted for credit monitoring services and insurance. *Id.* at *3. The pension fund sued the accountant to recoup the costs, who, in turned, tendered the defense of the suit to her homeowner's insurer. The homeowner's policy covered "property damage," which was defined as "physical injury to, destruction of, or loss of use of tangible property." Id. at *7. The policy also excluded "property damage" coverage "in connection with a business, under contract by the insured, or to property in the care of the insured." *Id.* at *13.

In surveying decisions made by other courts, the district court acknowledged that intangible losses are not considered "property damage," and the language of the definition plainly excluded the loss of use of "purely intangible property." *Id.* at *10. Nonetheless, the district court concluded that this is not a case where someone had hacked into the insured's

computer system and had erased the data or had stolen it without stealing the medium on which the information was recorded. Rather, the CD ROM—the medium on which the data was stored—was stolen. As such, the district court held that the insured "clearly suffered a 'loss of use' of that 'tangible property' when it was stolen from her car." *Id.* at *11. Despite this ruling, the district court went on to hold that the "in the care of the insured" exclusion had applied to bar coverage. The pension fund argued that the underlying complaint only alleged the insured came into possession of the CD-ROM and that it was in her car, which was parked outside her residence with no indication whether the car was actually on her property. As such, it argued these allegations were not sufficient to show possessory control, as required under the exclusion. The district court, however, rejected these arguments, concluding that the exact location of the car or the insured's knowledge were not relevant in order to trigger the exclusion. *Id*. at *15-16.

C. Crime Insurance

In 2012, the Sixth Circuit Court of Appeals in *Retail Ventures, Inc. v. National Union Fire Insurance Company of Pittsburgh, PA*, 691 F.3d 821 (6th Cir. 2012), sent shockwaves by finding coverage for a data breach under a blanket crime policy. In *Retail Ventures*, hackers gained unauthorized access to the insured's main computer system and downloaded credit card and checking account information belonging to more than 1.4 million customers of 108 stores, which the hackers used to conduct fraudulent transactions. As a result of the breach, the insured had incurred expenses for notifying the affected customers, public relations, customer claims and lawsuits, and attorney's fees in connection with investigation by seven state Attorney Generals and the Federal Trade Commission. *Id.* at 824. The insureds sought to recoup $6.8 million from AIG under an endorsement, entitled "Computer & Funds Transfer Fraud Coverage" ("Fraud Coverage Endorsement"), which insured losses "resulting directly from . . .[t]he theft of any Insured property by Computer Fraud. *Id.* at 826. The endorsement also contained an exclusion that precluded coverage "to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind."

The issue before the Sixth Circuit was whether the district court applied the correct standard below in finding that the words "resulting directly from" required a traditional proximate cause standard to trigger coverage under the Fraud Coverage Endorsement. AIG urged the Sixth Circuit to interpret this language narrowly, as requiring that the theft of property by computer fraud to be the "sole" and immediate cause of the insured's loss, thus precluding most of the insureds' damages. In other words, this language required a stricter causation standard than proximate cause because the word "directly" implied immediacy to the fraud.

The Sixth Circuit, however, disagreed with AIG, finding that the term "resulting directly from" did not limit coverage to loss "solely" to the theft itself. The Sixth Circuit also disagreed that the exclusion within the endorsement applied. The stolen customer information was not propriety information, since it was owned or held by many, including the customer, the financial institution, and merchants to whom the information was provided. The Sixth Circuit also refused

to interpret the catch-all phrase "or other confidential information of any kind" as including information belonging to anyone that is expected to be protected from unauthorized disclosures, as such an interpretation would "swallow not only the other terms in this exclusion but also the coverage for computer fraud." *Id.* at 833.

IV. Industry Response

The procurement of cyber liability insurance policies is expanding rapidly. This growth is undoubtedly caused by the increase of cyber risks and potential damages caused by the breaches. In addition, the recent decision in *Sony* has caused policyholders and underwriters to focus their attention on filling in the gap for cyber protection.

In fact, insurers have been "tightening the noose" for years around cyber-related risks. During 2001, the Insurance Services Office ("ISO") amended the definition of "property damage" in the standard CGL form so as not to include "electronic data." During 2004, ISO introduced a standard-form exclusion for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." During 2013, ISO introduced an optional endorsement that deletes the Coverage B "personal and advertising injury" offense of "oral or written publication of material that violates a person's right of privacy." Most recently, ISO introduced a new endorsement this year that bars coverage for "damages arising out of: (1) any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information, or any other type of nonpublic information; (2) or [t]he loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."

It is anticipated that ISO will continue to promulgate, and insurers will continue to adopt, policy definitions and exclusion that remove cyber-related risks for CGL policies. Furthermore, risk transfer down the chain of vendors may offer little recourse given the immense exposure created by a single cyber attack. Insureds with such exposures have little alternative but to seek risk transfer from the thriving cyber-liability insurance market.

Despite the increasing adoption of cyber liability policies, insureds commonly fail to procure insurance commensurate with their cyber-related risks. For example, in the *Sony* case discussed above, the Sony entities actually procured a cyber-risk policies, the scope of coverage for which reportedly encompassed aspects of the cyber attacks. Nonetheless, the limits of those policies were far below Sony's risk of exposure for the cyber attacks. Thus, with the recent trial court decision finding that the CGL primary insurers had no duty to defend Sony in the numerous underlying class action lawsuits, the lack of adequate limits with respect its cyber-risk program added substantial risk and costs to an already large problem.

As of this writing, numerous insurers offer cyber liability policies, i.e., policies specifically written to address risks attendant to cyber attacks. Limits of insurance on those

policies generally range from $10 million to $25 million. Many policies contain sub-limits for specific types of risks. At least one insurer, American International Group ("AIG"), is marketing a "CyberEdge PC" form that purports to be an add-on to an existing insurance program. The CyberEdge PC form provides for first-party coverage to the insured for crisis management response costs as well as third-party excess coverage and drop-down umbrella liability coverage. Thus, there are many products on the market, with an even broader array of risk transfer options for existing insurance programs or standalone coverage. A number of other insurers are also introducing multi-risk cyber programs with broad coverages and large limits. These programs come with very large premiums. It will be interesting to see if the policyholder market pursues these products.

Cyber liability policies generally offer risk transfer for both first and third-party losses. The most common types of risks transferred include:

- Losses resulting from claims by consumers whose personal data was stolen during a cyber attack (including defense and indemnity);
- Losses resulting from claims by businesses whose confidential business information was stolen during a cyber attack (including defense and indemnity);
- Losses resulting from claims by third parties that were required to outsource functionalities or capabilities provided by an insured;
- Losses incurred by the insured resulting from the introduction of malicious software on the insured's computer systems, denial-of-service attacks, appropriation of network code, destruction or corruption of data, theft of assets by a third-party, and disclosures of personal information by the insured's employees;
- Losses incurred for legal advice and representation in connection with regulatory investigations following a cyber attack (including the cost of fines and penalties);
- Losses incurred for forensic cyber risk specialists to investigate cyber attacks and determine whether data is missing and may be recovered;
- Losses incurred in recovering stolen data;
- Losses incurred for damage to its reputation (including crisis management and public relations "first responders");
- Losses incurred in complying with breach-notification laws and regulations;
- Losses incurred to compensate potential victims of a cyber attack, such as the establishment of credit monitoring and fraud insurance;
- Losses incurred due to the theft of intellectual property and trade secrets;
- Losses incurred due an interruption of the insured's computer networks; and
- Losses incurred due to extortion from cyber criminals.

A typical example is the NetProtect 360^{SM} product that has been marketed by CNA for several years. The third party liability coverage part insures "all sums" the insured becomes legally obligated to pay as damages resulting from a "Content Injury Claim," "Privacy Injury Claim," "Professional Services Claim," or "Network Security Claim" first made against the insured and reported to the insurer in writing during the policy period (or extended reporting

period) alleging a "Wrongful Act" by the insured or someone for whose "Wrongful Act" the insured is responsible. The form defines "Content Injury" and "Privacy Injury" similarly to the Coverage B offenses on the CGL form, though offering much broader coverage. Nonetheless the definition of "Wrongful Act" confines the scope of coverage to risks expected under a cyber liability policy.

The first party coverage part of the NetProtect360^{SM} form insures "all sums" that an insured incurs for: (1) "Network Extortion;" (2) loss of or damage to the insured's network; (3) reduction of business income suffered by the insured due to the interruption of "Commerce Operations;" (4) emergency responses expenses incurred from an "Exploit;" (5) losses resulting from "Electronic Theft" of the insured's money, securities, or goods; (6) "Electronic Theft" of "Services;" and loss of the insured's "Intangible Property." The form defines "Commerce Operations" to include the insured's income-producing activities. "Electronic Theft" includes transfer of the insured's money, securities, goods, intangible property to a person or entity not entitled to receive them. Significantly, the portion of the definition of "Electronic Theft" applicable to intangible property contains a clause deeming subsequent repetitions of the transfer to the same policy period. The definition of "Network Extortion" provides coverage for "credibly threatened" or received extortion demands made to the insured.

A key distinction among the first party coverages offered by the insurers lies in the type of coverage offered for crisis management costs incurred as a result of a cyber attack. Some policy forms require the insured to utilize specific crisis management service providers, while others simply offer discounted rates for utilizing a service provider recommended by the insurer. The policies vary in terms of the amount of time for which the crisis management benefit will be provided. Although these variances seem insignificant, the insured could incur a substantial uninsured loss if it fails to adhere to the policy terms by, for example, seeking reimbursement for an in-house crisis management response when the policy specifies a list of required or preferred crisis management vendors.

Cyber liability policies also vary in whether they offer media liability coverage. This coverage generally extends to any damages suffered by a third-party due to the insured's publication or failure to publish digital content as a result of a cyber attack. The coverage often extend to claims for:

- Defamation (libel, slander, and disparagement of trade reputation);
- Infringement of copyright, title, slogan, and trade name;
- Plagiarism, piracy, and misappropriation of ideas or information;
- Invasion, infringement, or interference with rights of privacy or publicity;
- Unfair competition; and
- Negligence.

It is important to note that cyber liability policies generally do not provide "all risk" coverage. In addition, cyber liability policies generally exclude the following risks:

- Antitrust violations, restraints on trade, or unfair competition not stemming from a cyber attack;
- Bodily injury and property damage;
- Contractual liability and warranty liability;
- Criminal acts, including acts or omissions found to be criminal or fraudulent by regulators;
- Disregard by company officers of court orders or regulator rulings;
- Difference in the quality, sensitivity, or value of data as disclosed to the insurer and data stolen or corrupted;
- Infringement of patents and trade secrets or loss of rights to secure registration to patents due to a cyber attack;
- Intentional acts by current or former directors, principals, partners, chief compliance officers, data protection officers, or general counsels;
- Failure to make royalty payments or license fees as a result of a cyber attack;
- Potential or actual claims existing prior to the policy's inception date;
- Violations of securities laws or regulations;
- War, terrorism, or riot;
- Trading losses or trading liabilities lost, diminished, or damaged as a result of a cyber attack;
- Unauthorized trading in excess of the insured's customary trading limits or in different product lines than the insured customarily trades in;
- Unauthorized collection of customer data;
- Unsolicited electronic mail, hardcopy mail, facsimiles, audio, video, or telemarketing; and
- Non-insurable losses (e.g., punitive damages in certain jurisdictions).

In addition to the above exclusions, a common condition of cyber liability coverage is that the insured maintain the security of its network. For example, one specimen form issued by AIG requires the insured to "take all reasonable steps to maintain data and information security procedures to no lesser standard than disclosed in the proposal form." The phrase "all reasonable steps" is not defined by the form. Presumably, an insured must adhere to "industry best practices" with respect to the maintenance of its network, in addition to disclosing to the insurer which specific steps will be undertaken in order to secure its computer networks. Another trap within which insureds may fall is incurring defense-related expenses without prior authorization or approval from the insurer. *See Gulf Underwriters Ins. Co. v. Nucentrix Broadband Networks, Inc. (In re Nucentrix Broadband Networks, Inc.)*, 309 B.R. 907, 910 (Bankr. N.D. Tex. 2004) (finding that an insurer had no duty to reimburse defense costs incurred by the insured because the cyber liability policy required prior authorization and approval from the insurer with respect to coverage for defense costs).

At present, several insurers are marketing a product that offers insureds a potential defense against cyber attacks. For example, AIG offers "qualified clients" a hardware component that can be embedded in a company's IT infrastructure. The devise "isolates and

shuns bad IP addresses, preventing them from entering and exiting a company's network." The device is aimed at quashing denial-of-service attacks and thwarting the transfer of malicious code from known "bad" IP addresses. AIG also offers free cyber threat alerts to its customers and potential customers via an iPad app.

V. Conclusion

In sum, insurers have become quite active in the cyber liability market, which is experiencing significant expansion at present. Significantly, insurers and courts have been placing increasing pressure on insureds not to look for risk transfer for cyber-related risks under CGL policies. With coverage so uncertain under CGL policies and an increase in cyber attacks and other cyber-related risks identified above, the recent expansion of the cyber liability market will continue to grow for the foreseeable future.