ABA Section of Litigation 2012 Insurance Coverage Litigation Committee
Women In Insurance Networking Workshop,
October 18, 2012:
Cloud Cover: Insuring Technology & Cyberliability Risks

Cloud Cover: Insuring Technology & Cyberliability Risks

Nancy D. Adams
Mintz Levin PC
Boston, MA

Elissa K. Doroff
Marsh USA Inc.
New York, NY

Mary E. McCutcheon
Farella Braun & Martel LLP
San Francisco, CA

Stacey L. McGraw
Troutman Sanders LLP
Washington D.C.

CLOUD COVER: INSURING TECHNOLOGY & CYBERLIABILITY RISKS

By now, surely everyone has received a letter from a major financial institution, a health care provider or a university that you once attended explaining that some of your personal identifying information has been put at risk. Whether caused by a hacker who seeks the

information for an identity theft scheme, or just an employee who left a laptop in a taxi, these "data breach" events are a well-known risk for any company or institution that collects personal data about its customers or employees. In response, many insurance companies are now offering "cyber liability" or "cyber risk" policies designed to protect against data breaches and other electronic injuries that companies can either suffer or cause to others. With recent SEC guidance that companies ought to disclose how they protect themselves against these types of risks and potential liabilities, demand for cyber liability policies is continuing to increase. This article reviews the types of policies that may or may not provide coverage and explores how, despite the distinctly new risks that these policies address, we can expect familiar coverage issues to drive the disputes that may arise between insureds and insurers.

Nearly All Companies Face These Issues

According to Verizon's 2012 data breach investigations report, the finance and insurance industries experienced the largest percentage of data breaches followed closely by information technology, retail trade, manufacturing, public administration, transportation and warehousing as well as education, government, and healthcare. It seems that almost no one is immune to this danger.

Why are certain industries targeted more than others? The retail sector is a large target because retailers store Personally Identifiable Information ("PII") data that is not always protected through firewalls or encryption. Similarly, the health care industry is a big target because of the storage of Personal Health Information ("PHI"). In general, healthcare, financial, and retail sectors that store records containing PII, PHI and credit card information are most at risk, with hackers and rogue employees as well as contractors responsible for the majority of data losses. Notably, human error (i.e., the laptop left behind at the airport) remains a large cause for data loss as well.

Increased regulations such as the Health Information Technology for Economic and Clinical Health Act ("HITECH") are driving the next wave of third-party lawsuits. Passed in February 2009, HITECH significantly expanded the Health Insurance Portability and Accountability Act (HIPAA) regulations and increased penalties for violations. Under HITECH, HIPAA rules now apply to the "business associates" of HIPAA-covered entities. These "business associates" must now have written policies and documentation of security safeguards in place. In addition, the act imposed a new mandatory federal security breach reporting requirement and created new privacy requirements including new accounting requirements for electronic health records.

HITECH also established new criminal and civil penalties for noncompliance along with new enforcement responsibilities. The civil penalties increased from just $100 per violation (up to $25,000 per identical violation) to between $100-$50,000 for each violation (up to $25,000 to $1,500,000 per identical violation) and that is only for cases where the violation was doing unknowingly. For violations attributable to "reasonable cause" but not "willful neglect," the civil penalties range from $1,000 to $50,000 per violation (up to $100,000 to $1,500,000 per identical violation). For violations caused by

willful neglect, they range from $10,000 to $50,000 for each violation (up to $250,000-$1,500,000 per identical violation). These penalties may increase, however, if the violation is not corrected within 30 days of discovery. HITECH also gives enforcement authority to the State Attorneys General and allows states to seek the award of attorneys' fees.

In addition to HITECH, companies face a regulatory environment that has become increasingly stringent in the past few years, including compliance with Sarbanes-Oxley, state privacy breach notification laws, and the standards imposed by the credit card associations, known as Payment Card Industry ("PCI") standards. These PCI standards must be adopted by all organizations that store, process, or transmit cardholder data. PCI standards require these organizations to build and maintain a secure network, protect cardholder date through encryption, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy.

In addition, there are data breach notification laws in nearly every state and the following regulations also create additional requirements:

- The Gramm-Leach-Bliley Act ("GLBA") – Signed into law in 1999, the GLBA governs financial institutions that collect nonpublic personal information. The act requires those institutions to provide initial and annual privacy notices, restricts how and when they may disclose information to third parties, and allows consumers to "opt out" if they do not want their information shared.

- The Fair and Accurate Credit Transactions Act ("FACTA") – Enacted in 2003 to reduce the risk of identity theft by regulating how consumer account information is handled.

- Red Flag Identity Theft regulations – Implemented by the FACTA enforcement agencies. Require financial institutions and creditors to develop and implement a written Identity Theft Prevention Program. The program must identify red flags that may arise in the handling of consumer data by employees and be updated periodically to reflect new identity theft risks.

- SEC guidance – In October 2011, the SEC issued a guidance to public companies regarding their disclosure obligations in connection with cybersecurity risks and cyber incidents.

- California's Song-Beverly Credit Card Act – Limits ability of retailers to request or record personal information in connection with credit card transactions. Violators are subject to civil penalties not to exceed $250 for the first violation and $1000 for each subsequent violation.

- California's "Shine the Light" Act - Applies to all companies that do business in California and requires them to either allow customers to opt out of information

sharing or make a detailed disclosure of how personal information is shared for direct-marketing purposes. Also creates a private and unwaivable cause of action, which includes statutory penalties ranging from $500 to $3000 per violation.

- The EU Data Protection Directive - Broader than U.S. laws and seeks to implement one uniform notification standard. Creates rights for people about whom information is collected and imposes strict rules on companies that want to use that information in direct marketing or transfer it to other companies. In January 2012, the European Commission unveiled a draft European Data Protection Regulation that may supersede the directive.

Data Breach Coverage Provides Key Protection For Third-Party and First-Party Losses

The most prominent problem against which a cyber liability policy aims to protect is the data breach, where a malicious hacker or a negligent employee puts either company or customer information at risk. A recent study of data breaches analyzing claim payouts concluded that the average loss is $2.4 million per data breach event, a number that does not include the first party expenses of the organization that suffered the breach. While a data breach can involve lost customer data, lost company data (such as intellectual property), and/or lost employee data, the risks for which cyber risk policies can provide coverage often include other types of cyber-related events. For example, another common problem is an organization receiving a computer virus, or passing along the same to a customer or other third-party, which itself can cause a loss of data or an inability to use computer systems. Unfortunately, overzealous or rogue employees also are a source of risk, and they can cause trouble by slandering a competitor via social media, gaining access to another company's electronically-stored information, or infringing on copyrighted materials.

An organization facing a data breach, or any other type of cyber risk, is likely to incur multiples types of damages. In the event of lost third-party data, most states now have regulations governing how a company must provide notice to its customers (hence, the letters we receive all too frequently informing consumers that personal information may be at risk), as well as the possibility of penalties for failing to protect data. Almost inevitably, there will be lawsuits, with the substantial costs that those entail. If the company's own data is at risk – through a data breach or malware attack – the organization will need to take steps to replace or protect its data and often will suffer losses associated with an interruption to its business. In other words, cyber risks can entail significant first- and third-party losses.

When a third party is involved, a company may be faced with a substantial exposure. Where previously plaintiffs had to prove actual harm or damages to establish standing, courts have begun to consider data breach litigation in the same light as toxic tort litigation. In other words, the threat of a future injury (identity theft) might be enough to establish damages, just as the threat of a future medical condition in a toxic tort case is sufficient to establish damages (i.e., Asbestos). *Anderson v. Hannaford Bros.*, No. 10-

2384 and No. 10-2450 (1st Cir., Oct. 20, 2011) (court reinstated negligence and implied contract claims brought on behalf of plaintiffs whose financial data was compromised based on the theory that it was reasonably foreseeable that plaintiffs whose personal information was misused would have to take action to protect themselves); *Pisciotta v. Old National Bancorp*, 499 F.3rd 629 (7th Cir. 2007); *Krottner v. Starbucks Corp.*, 628 F.3rd 1139 (9th Cir. 2010).

In addition, cause does not matter. Since a regulatory action usually precedes a civil action, substantial legal and forensic investigation costs can be incurred even for events where no one is harmed or even at risk. For companies processing credit card data, compliance with the PCI standards definitely helps to drive security but will not necessarily defeat a claim for negligence. As a result, any claim involving third parties can be extremely expensive and time-consuming to resolve.

Traditional Policies May Not Provide Right Type of Coverage

For companies with potential cyber risks, it is not a safe bet to rely on traditional policies to provide coverage. Claims for coverage under standard commercial general liability policies often are unsuccessful due to an inability to demonstrate property damage, which requires injury to tangible property, a threshold that damage to electronic data generally does not meet. In addition, such property damage must be the result of an occurrence not caused by intentional acts to be covered under the typical general liability policy, and many data breaches and other cyber risks involve hackers and other criminal actors engaged in intentional wrongdoing. Insureds also sometimes seek coverage for advertising injury, but that usually requires publication; lost data is (thankfully for us as consumers) often not seen by anyone. Still, whether a general liability policy provides coverage for these types of risks depends on the individual policies and the nature of the particular harms, so coverage disputes remain common.

Insureds may run into similar problems seeking coverage under errors and omissions policies. A typical professional liability policy requires that insureds engage in a wrongful act, usually in connection with work performed for a customer. If a company's professional services involve handling data or other tech-related activity, there is a greater likelihood of coverage under an E&O policy. For example, in *Eyeblaster, Inc. v. Fed Ins. Co.*, 613 F.3d 797 (8th Cir. 2010), the insured, an online marketing campaign management company, was sued by an individual who alleged that the insured's online advertising caused his computer to be infected with a spyware program that severely impaired the function of his computer, resulting in data loss, numerous pop-up ads, a hijacked browser, and frequent error messages. The Eighth Circuit found that the allegations triggered a duty to defend under the E&O policy because Eyeblaster's activity of causing software (such as Flash and JavaScript) to be installed on the computer, while intentional, was not an intentional wrongful act. See also *Tagged, Inc. v. Scottsdale Ins. Co.*, No. JFM-11-127, 2011 U.S. Dist. LEXIS 75262 (S.D.N.Y. May 27, 2011) (a professional services exclusion in a D&O policy applied to allegations that a social networking site's management falsely represented the level of protection afforded to children on their site because the allegations involved the professional service of

regulating the content of the website). However, in *New Fed Mortg. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, 543 F.3d 7 (1st Cir. 2008), the insurer had no duty to defend allegations that an employee of the insured falsified personal information in electronic credit reports as part of mortgage applications because intentional misconduct was excluded from coverage. Thus, for issues related to data security provided to clients and online interactions with third-parties, a standard E&O policy might provide some coverage, at least in responding to claims. By contrast, in the typical data breach scenario, many of the costs incurred by the victim company are either first-party losses or involve activity under taken prior to a "claim" being made, including providing notice to parties at risk and otherwise complying with government regulations. Therefore, while an insured may be able to obtain reimbursement of litigation expenses, notice and compliance costs are likely not within the coverage of a typical professional liability policy.

For intentional wrongful acts not covered by CGL and professional liability policies, insureds can sometimes turn to commercial crime policies, but the common policy forms in that area also include limitations that may pose problematic in the typical cyber risk event. Specifically, such policies may exclude indirect or consequential loss of any kind, as well as the loss of "future" income, which likely would limit an insured's ability to recover its own losses.

In addition, such policies may try to exclude loss caused by the theft of confidential information, which drives much of the costs and litigation arising from cyber risk. The U.S. Court of Appeals for the Sixth Circuit recently addressed this type of exclusion, holding that there was coverage for first-party and third-party losses arising from the theft of customer credit card information by hackers under a crime policy's computer fraud endorsement. See *DSW Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa.*, Case No. 10-4576/5608 (Aug. 23, 2012). The Sixth Circuit found that the crime policy at issue covered third-party liability losses even though the insuring agreement limited coverage to loss "resulting directly from" the "theft of any Insured property by Computer Fraud." The Sixth Circuit also refused to apply an exclusion barring coverage for "any loss of proprietary information, Trade Secrets, Confidential Processing Methods or other confidential information of any kind." The court reasoned that, while credit card information might be considered confidential in some circumstances, it could not have been the type of confidential information envisioned by the exclusion. Otherwise, the exclusion would vitiate the coverage that the policy promised to provide. While the court found that this particular claim was covered, the decision further emphasizes the importance of reading the insuring agreements and exclusions of each policy carefully.

Coverage Is Becoming More Common But There Is No Standard Policy Language

In light of the uncertainty of whether the typical menu of available coverage will cover losses from cyber risks, demand for insurance policies specifically designed for these events continues to grow. This demand has increased with the SEC Division of Corporate Finance's Disclosure Guidance on Cybersecurity, issued on October 13, 2011. The Disclosure Guidance recommended that companies should disclose the risk of cyber

incidents for their particular business, as well as what steps the company takes to address those risks, including a description of the relevant insurance coverage. While not creating an official requirement to purchase cyber liability insurance, after the SEC specifically identified this as a concern, more companies are becoming aware of the issue, including the litigation risks if they are not properly insured. The SEC Disclosure Guidance raises the question of whether the failure to purchase cyber liability insurance can open a company up to D&O claims for breach of fiduciary duty or securities violations for not adequately protecting the company against such risks if a cyber liability event occurs, or for not disclosing to shareholders knowledge of inadequate protections or ongoing risks.

Even though some of these issues are still relatively new, the risks are well-known and there are now a number of examples where insurers have provided substantial coverage for these types of losses. For example, carriers have covered claims where hackers have stolen credit card information and passwords. Carriers have also covered claims involving employees where records were stolen and sold or where the employee misappropriated confidential information from a competitor. Coverage has also been found where the insured simply lost or accidentally published confidential information.

While specific cyber liability policies – or endorsements to GL or E&O policies addressing these risks – have been available for a few years, they are still in their relative infancy, without the standardization that is typical of policy forms in some more well-established areas. Third-party cyber liability coverage can include protection against liability for permitting access to identifying information of customers (including information stored by third parties on your behalf), transmitting a computer virus or malware to a third party customer or business partner, or failing to notify a third party of their rights under the relevant regulations in the event of a security breach. Such policies also can cover "advertising injury"-like harms through the use of electronic media, such as unauthorized use or infringement of copyrighted material, as well as libel, slander, and defamation claims. First-party cyber liability coverage can include paying for the costs of providing notice to individuals whose identifying information was compromised; determining the scope of the breach and taking steps to stop the breach; obtaining public relations services to counteract the negative publicity that can be associated with a data breach or other cyber risk losses; reimbursing the costs of responding to government investigations; and reimbursing the costs of replacing damaged hardware or software and replacing data. In addition, some companies offer reimbursement for damages to the insured entity caused by computer fraud; reimbursement for payments made to parties blackmailing the company or the costs of responding to parties vandalizing the company's electronic data; and business interruption costs.

Expect Familiar Issues To Arise In Coverage Disputes

Although the new forms of cyber liability coverage address protecting data and using electronic media to communicate – risks associated with modern methods of doing business – traditional coverage issues are still likely to drive disputes between insureds and insurers. For example, the insured will have to consider its obligations to provide

notice of circumstances, as well as notice of claims, in these new circumstances. What aspects of a company's cyber risk must be disclosed on an application? Does a known weakness in cyber security constitute circumstances that could lead to a claim? With whom does a company's risk manager need to speak to determine whether circumstances that could lead to a claim exist? In-house, will the Chief Technology Officer need to learn what constitutes a potential claim under various insurance policies? Are there any vendors or other third parties who are responsible for a company's data that must be asked about potential claims? Then, once there is a cyber liability event, how soon must it be reported to the carrier? Since occurrences such as a data breach are often public relations crises, what happens to coverage in the event of a delay in reporting or if the company takes action before involving its insurer? Companies will have to grapple with these issues, particularly when completing applications for insurance and when analyzing possible flaws in security measures, while carriers similarly will have to consider how much information they will require about a company's security efforts in order to measure the risk of providing coverage.

Of course, addressing new types of coverage – particularly ones that are not standardized – almost certainly will lead to questions about the scope of covered loss. For example, a New Jersey federal district court recently ruled, on a motion to dismiss, that a policy may provide coverage for hackers who took over the servers of Vonage (an internet calling company), causing the insured to lose the ability to process calls, its source of profit. *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, Civ. No. 11-6187, 2012 U.S. Dist. LEXIS 44401 (D.N.J. Mar. 29, 2012). The relevant coverage language stated that the insurer

> will pay for loss of and loss from damages to 'money', 'securities' and 'other property' following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the 'premises'...

The carrier argued that a "transfer of that property" required the property to be physically taken, but the court rejected the argument and ruled that the "transfer" referenced in the policy language could be temporary, so the insurer's motion to dismiss was denied.

Policyholders and carriers also may debate whether multiple cyber liability claims are related, which can affect whether a claim falls within a particular policy period. In *United Westlabs, Inc v. Greenwich Ins. Co.*, the Delaware Superior Court ruled that the claims against the insured – which involved both a cyber risk (a "cyber extortion threat"), as well as a lawsuit potentially triggering coverage under a private company reimbursement policy – were related to claims preceding the policy period because the wrongful acts at issue in the matters were fundamentally identical. The court rejected the insured's argument that the earlier claim was resolved, and thus based on separate events, and the argument that two acts were not interrelated because they involved different actions (e.g., the insured itself doing the "hacking," versus a third party retained by the insured to commit the wrongful act). No. 09C-12-048, 2011 Del. Super. LEXIS 261 (Del. Sup. Ct. June 13, 2011). Thus, the related claims language of both the policy

covering cyber risk and the traditional private company reimbursement policy applied to preclude coverage.

Insurers also will need to determine how cyber liability policies interact with other types of insurance policies when both potentially respond to a particular incident. In other words, intra-insurer disputes over allocation may have a new variable. For example, in the *United Westlabs* case, if, instead, both the policy responding to the cyber extortion threat and the traditional liability policy provided coverage, how would the carriers divide up the defense and the indemnity obligations? How likely is it that the coverages will overlap? If they do, which policy would provide first dollar coverage and how would loss be allocated between the two policies? For example, in *United Westlabs*, if the litigation against the insured concerned the cyber extortion threat, would the cyber liability carrier be responsible to pay for part of the litigation?

We could spin out these hypotheticals all day, but the problems that may arise are ones that would look familiar to any coverage lawyer. However, it likely is time to start thinking about how these "old" issues will intersect with 21st century technology and a still-developing set of policies designed to protect against cyber risk.

Appendix A

Security & Privacy Insurance Policy Coverage Overview

Not covered	Covered	See notes	Dependant upon specifics of claims, maynot be covered

Privacy & Cyber Perils	Property	General Liability	Traditional Fidelity Bond	Computer Crime (not purchased - only for FIs)	E&O (not purchased))	Special Risk	Broad Privacy & Cyber Policy
Destruction, corruption or theft of your electronic information assets/data due to failure of computer or network							
Theft of your computer systems resources							
Business interruption due to a material interruption in an element of your computer system due to failure of computer or network security (including extra expense and forensic expenses)							
Business interruption due to your service provider suffering an outage as a result of a failure of its computer or network security							
Indemnification of your notification costs, including credit monitoring services							
Defense of regulatory action due to a breach of privacy regulation							
Coverage for Fines and Penalties due to a breach of privacy regulation							
Threats or extortion relating to release of confidential information or breach of computer security							
Liability resulting from disclosure of electronic information & electronic information assets							
Liability from disclosure confidential commercial &/or personal information (i.e. breach of privacy)							
Liability for economic harm suffered by others from a failure of your computer or network security (including written policies & procedures designed to prevent such occurrences)							

BA Section of Litigation 2012 Insurance Coverage Litigation Committee
Women In Insurance Networking Workshop,
October 18, 2012:
Cloud Cover: Insuring Technology & Cyberliability Risks – Key Cases

Cloud Cover: Insuring Technology & Cyberliability Risks – Key Cases

Nancy D. Adams
Mintz Levin PC
Boston, MA

Mary E. McCutcheon
Farella Braun & Martel LLP
San Francisco, CA

Stacey L. McGraw
Troutman Sanders LLP
Washington D.C.

CLOUD COVER: INSURING TECHNOLOGY& CYBERLIABILITY RISKS – KEY CASES

I. Cyber Liability Cases Involving General Liability Policies

Connecticut
Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., No. X07CV095031734S, 2012 Conn. Super. LEXIS 227 (Conn. Super. Ct. Jan. 17, 2012)
The insured, who had contracted with IBM to provide distribution services, sought coverage under its general liability and umbrella policies when an IBM cart holding computer data tapes fell out of a transport van on a highway ramp and was taken by an unknown third person. The tapes contained personal data for more than five hundred thousand IBM employees. The insured claimed that when the tapes were stolen, both property damage and publication had occurred, and that the claims made by

IBM were covered under its policies. The court rejected these arguments, noting that IBM did not seek damages for the tapes or the cart, but had rather made claims for the loss of electronic data, which could not be construed as damage to tangible property as required by the definition of property in the policies. Further, the court held that there was no publication, as publication requires evidence of communication to a third party, which was not present in the case.

Louisiana

Union Pump Co. v. Centrifugal Tech., Inc., No. 05-0287, 2009 U.S. Dist. LEXIS 86352 (W.D. La. Sept. 18, 2009)

In this case, the court found that there was no coverage under the insured's commercial general liability policy for litigation involving claims that the insured had wrongfully used and then destroyed electronic data which included plaintiff's design drawings, autocad drawings, and pump models. As to coverage for property damage, the court found that electronic data failed to meet the definition of "tangible property" as required by the policy and that further, coverage only applied to property damage in the event of an "occurrence." Since plaintiff's claims all involved allegations of intentional acts, they were excluded under the intentional act exclusion. With respect to personal and advertising injury, the court found that no evidence was presented that the insured had engaged in any act of advertisement that would be consistent with the policy.

Minnesota

Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010)

The insured, an online marketing campaign management company engaging in rich media advertising, was sued by an individual who alleged that the online advertising caused his computer to be infected with a spyware program which severely impaired the function of his computer, resulting in data loss, numerous pop-up ads, a hijacked browser, and frequent error messages. The insurer denied coverage under the general liability policy because the complaint did not assert claims for bodily injury or property damage to tangible property caused by an accident or occurrence as required by the policy. The insurer also denied coverage under a technology E&O policy, claiming that the plaintiff in the underlying action had failed to allege that the insured had committed a wrongful act (defined in the policy as an error, unintentional omission, or a negligent act) in connection with a product failure or in failing to perform service. The court found that the action was covered both under both policies. With the regard to the general liability policy, the court found that while damage to software would not have been covered under the policy, the loss of use of the computer, which was tangible property, was sufficient. Further, under the E&O policy, the court found that "error" in a technology E&O policy "to include intentional, non-negligent acts but to exclude intentional wrongful conduct," which encompassed the insured's actions.

II. Cyber Liability Cases Involving E&O Or D&O Policies

Delaware

United Westlabs, Inc. v. Greenwich Ins. Co., No. 09C-12-048 MMJ, 2011 Del. Super. LEXIS 261 (Del. Super., June 13, 2011), *aff'd* No. 337, 2011, 2012 Del. LEXIS 130 (Feb. 28, 2012)

Under a policy covering liability for cyber and technology activities, coverage was barred for an action filed against the insured during the policy period because the wrongful acts alleged were part of a continuous series of related acts that had been alleged in an action filed before the policy inception.

Massachusetts

New Fed Mortg. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, 543 F.3d 7 (1st Cir. 2008)

A residential mortgage originator sought to compel the insurer to provide coverage and defense costs under its E&O policy after an employee of the insured falsified electronic credit reports in several

mortgage applications. The court held that the insurer had no duty to defend because the underlying litigation involved allegations of intentional misconduct that were plainly excluded from coverage.

Minnesota

St. Paul Fire and Marine Ins. Co. v. Compaq Computer Corp., 539 F.3d 809 (8th Cir. 2008)

Applying Texas law, the Eight Circuit found that the insurer had a duty to defend under a technology E&O policy because the allegations in the underlying litigation included conduct falling within the policy's definition of "error." Specifically, the plaintiffs alleged the insured engaged in the unintentional incorrect act of selling defective computers. As the act was alleged to be unintentional rather than intentional, the claims fell within the scope of the policy.

New Jersey

Vonage Holdings Corp. v. Hartford Fire Ins. Co., Civ No. 11-6187, 2012 U.S. Dist. LEXIS 44401 (D.N.J. Mar. 28, 2012)

The insured sought coverage under a cyber liability policy after a group of computer hackers accessed the insured's servers and used them to route calls to Cuba through one of the insured's telecommunications partners. The policy provided coverage for damage to money, securities, and other property "following and directly related to the use of any computer to fraudulently cause a transfer [to a person or place outside the premises]." The insurer sought to dismiss the insured's action, claiming that the insured had not alleged that tangible property directly related to the use of a computer was transferred outside the premises and that the insured had failed to allege "loss of" or "loss from damage to" tangible property. The court denied the insurer's motion to dismiss, finding that the policy language was ambiguous and that defendant's reading of the provision was reasonable. The case is pending.

New York

Tagged, Inc. v. Scottsdale Ins. Co., No. JFM-11-127, 2011 U.S. Dist. LEXIS 75262 (S.D.N.Y. May 27, 2011)

Under California law, the court held that a directors and officers policy issued to a social networking website excluded coverage for a claim alleging that the website's management falsely represented the content protections for children because the allegations involved the professional service of regulating the content of the website.

III. Cyber Liability Case Involving A Crime Policy

Ohio

DSW Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa., Case No. 10-4576/5608 (Aug. 23, 2012).

The U.S. Court of Appeals for the Sixth Circuit recently addressed an exclusion for loss caused by the theft of confidential information. The court found that there was coverage for first-party and third-party losses arising from the theft of customer credit card information by hackers under a crime policy's computer fraud endorsement. The Sixth Circuit found that the crime policy at issue covered third-party liability losses even though the insuring agreement limited coverage to loss "resulting directly from" the "theft of any Insured property by Computer Fraud." The Sixth Circuit also refused to apply an exclusion barring coverage for "any loss of proprietary information, Trade Secrets, Confidential Processing Methods or other confidential information of any kind." The court reasoned that, while credit card information

might be considered confidential in some circumstances, it could not have been the type of confidential information envisioned by the exclusion. Otherwise, the exclusion would vitiate the coverage that the policy promised to provide.

IV. Pending Cyber Liability Cases In The News

Arch Ins. Co. v. Michaels Stores Inc., 1:12-cv-00786 (N.D. Ill. filed Feb. 23, 2012)

Arch brought suit seeking a declaration that it is not required to indemnify or defend Michaels under a general liability policy in connection with a recent security breach where criminals known as "skimmers" tampered with PIN pad terminals in Michaels stores, using them to steal customers' financial information and obtain access to their bank accounts. Arch asserts that none of the underlying suits allege property damage, bodily injury, or advertising injury, as required by the policies. Moreover, Arch contends that the electronic data and breach of contract exclusions in the policies apply.

Zurich Am. Ins. v. Sony Corp. of Am., No. 651982/2011 (N.Y. Sup. Ct. filed July 20, 2011)

In April 2011, hackers accessed data for one hundred million Sony PlayStation users and as a result, Sony was sued in sixty actions across the United States. Zurich brought suit seeking a declaratory judgment, claiming that it has no duty to defend or indemnify Sony against customer class actions and related matters. Sony purchased primary commercial general liability and excess liability policies from Zurich. Zurich asserts that the lawsuits arising out of the cyber attacks are not covered by the "bodily injury," "property damage" and "personal and advertising injury" coverage provided by its liability policies.