

Risky Business with Cyber Insurance – Sunglasses Not Optional

American Bar Association Section of Litigation
Insurance Coverage Litigation Committee
March 1-4, 2017

Lori L. Siwik
Founder and Managing Partner



Jason Warmbir
Vice President
FINEX Cyber Liability Practice



Dorothea W. Regal
Partner



Ray Wong
Partner



Kathryn Kasper
Director



Introduction

Data breaches have resulted in hundreds of millions of data records being illegally accessed. Home Depot, Target, Michael's, TJ Maxx, Snapchat, Facebook, Twitter, Sony, Kmart, Apple's iCloud, First Commonwealth Bank, and P.F. Chang's are just a few of the companies that have reported a major data breach. The Russian hacking of the Democratic National Committee during the 2016 Presidential campaign may have impacted the election. Similarly, DDos (Denial of Service) attacks have targeted banks and other financial service providers.

According to the Verizon 2016 Data Breach Investigation Report, 89% of breaches had a financial or espionage motive. The attackers hacked, distributed malware, phished and instituted social engineering schemes to get access to the data. Employee negligence also played a role in data breaches with lost and stolen devices, as well as through the use of portable devices such as cell phones, laptops, iPads, flash drives, and other devices – all of which pose a security risk to companies and their computer networks.

Every company, large or small, is susceptible to a data breach. With more and more companies using technology to manage their daily business activities, it is becoming easier for criminals and non-criminals to get access to sensitive information like social security numbers, bank account information, credit card numbers and intellectual property information. Data breaches can cost a company millions of dollars in defense and settlement costs arising from the breach, in business interruption expenses, and in damages to remedy the breach itself. Losses arising from data breaches average \$158 per lost record with an average total cost of \$4 million per company.¹

What are the Data Breach Laws?²

Data breach notification laws have been enacted in every state, but the requirements vary from state to state. These data breach notification laws are triggered when there has been a breach of personal information, which is not uniformly defined in the statutes. What to include in the notification can have negative consequences to the company reporting the breach. For instance, in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), Neiman Marcus followed state law and reported that 9200 credit cards had experienced fraud and that customer credit reports should be reviewed. The Seventh Circuit relied on the notice statements when ruling that the plaintiffs had met the requirements for a class action. Similarly, in *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), P.F. Chang's publicly announced its data breach before it knew the complete scope of the breach without indicating that not all its locations were affected and may have implied that all were by its action of temporarily installing a manual card-processing system at all its locations. After announcing the breach, it learned that only 33 restaurants had been affected by the breach. In the Seventh Circuit appeal, P.F. Chang's argued that the named plaintiffs in the class action suit had no standing to bring the class action because they were not customers at any of the 33 affected restaurants. The Seventh Circuit rejected this argument, relying on the early notice that P.F. Chang's had provided to all of its customers.

¹ Ponemon Inst. 2016 *Cost of a Data Breach Study*: available at <http://www-03.ibm.com/security/data-breach>

² Recently, Mayer Brown published a guide, "Cybersecurity Regulation in the United States: Governing Frameworks and Emerging Trends." The guide is an excellent resource.

The FTC, under Section 5 of the Federal Trade Commission Act, has authority to protect consumers from unfair or deceptive data security practices and does so by instituting enforcement actions.³ The FTC holds a breached entity accountable for meeting a data security level that is “reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.”⁴

The Securities and Exchange Commission’s Division of Corporate Finance guidance on cybersecurity disclosures provides, per the federal securities laws, that companies “should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents” and that “appropriate disclosures may include,” a “[d]escription of relevant insurance coverage. See www.sec.gov/divisions/corpfin/guidance.

Is There Insurance Available for Data Breaches?

Companies may receive lawsuits seeking damages as a result of a data breach. Claims of invasion of privacy, lost or stolen data, loss of use of computers, misappropriation of confidential business information, etc. can cost companies thousands of dollars to defend. Governmental and regulatory actions related to data breaches are also common.

When faced with a data breach or an electronic data loss, many companies may look to their commercial general liability (“CGL”) policies and first-party property policies for coverage. A dispute often arises between the insurance carrier and the policyholder regarding the availability of coverage.⁵

Sometimes the battle is over whether there is a privacy violation or a publication such that there would be coverage under CGL policies.⁶ See *Zurich Am. Ins. Co., v. Sony Corp. of Am.*, 2014 N.Y. Misc. LEXIS 5141 (2014); *Hartford Cas. Ins. Co. v. Corcino & Assocs.*, 2013 U.S. LEXIS 152836 at *12 (C.D. Cal. Oct. 7, 2013) (the court rejected the insurance carrier’s argument that the personal injury coverage excluded claims for disclosure of personal data of hospital patients, and observed that “medical records have been considered private and

³ In *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp.3d 602 (3rd Cir. 2014), the Third Circuit Court of Appeals held that the FTC has authority to bring enforcement actions against companies relating to their data security practices.

⁴ “Privacy Law: Protecting the Good, the Bad and the Ugly: “Exposure” Data Breaches and Suggestions for Coping with Them”, Yasmine Agelidis, 31 Berkeley Tech. L. J. 1057 (2016), citing “Data Security, Fed. Trade Comm’n, <https://www.ftc.gov/datasecurity>

⁵ An excellent article that discusses insurance coverage for cyber attacks is “Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of the Internet” by Roberta D. Anderson, 49 Tort & Ins. L.J. 529 (Winter, 2014). See also “Claims Made and Insurance Coverage Available for Losses Arising Out of or Related to Electronic Data”, by Jeffrey S. Price and Justin D. Wear, 51 Tort & Ins. L.J. 51 (Fall, 2015) and “Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today’s Litigation and Tomorrow’s Challenges”, by Gregory D. Podolak, 33 Quinnipiac L.Rev. 369 (2015).

⁶ The 2007 and later ISO insurance forms contain an exclusion for privacy-related laws.

confidential for well over 100 years at common law”); *Recall Total Info. Mgmt. v. Fed. Ins. Co.*, 83 A.3d 664 (Conn. App. 2014), *aff’d*, 115 A.3d 458 (Conn. 2015); *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC*, 35 F. Supp.3d 765 (E.D. Va. 2014); *Pietras v. Sentry Ins. Co.*, 2007 U.S. Dist. LEXIS 16015 (N.D. Ill. Mar. 6, 2007); *Valley Forge Ins. Co. v. Swiderski Elecs., Inc.*, 860 N.E.2d 307 (Ill. 2006); *Zurich Am. Ins. Co. v. Fieldstone Mortgage Co.*, 2007 U.S. Dist. LEXIS 81570 (D. Md. Oct. 26, 2007); *Park Univ. Enters., Inc. v. Am. Cas. Co.*, 442 F.3d 1239 (10th Cir. 2006); *Columbia Cas. Co. v. HJAR Holding, LLC*, 411 S.W.3d 258 (Mo. 2013).

Often the battle is over whether there has been “property damage”. In many insurance policies “Property Damage” is defined as “physical injury to tangible property, including all resulting loss of use of that property” and “loss of use of tangible property that is not physically injured.”⁷ Insurance carriers argue that electronic data is excluded from the definition of tangible property. See *Arch Ins. Co. v. Michaels Stores, Inc.*, No 12-00786 (N.D. Ill. Feb. 3, 2012). Many courts find that data does not amount to “tangible property” because computer information lacks physical substance. See *Ward Gen. Servs. Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 556-57 (Cal. App. 4 Dist. 2003) (where a computer crash, due at least in large part to human operator error, resulted in data loss, the court held that there was no physical loss or damage. The court held that data loss was simply a “loss of organized information . . . (such as client names and addresses). . . .” concluding that such information “cannot be said to have a material existence, be formed of tangible matter, or be perceptible to the sense of touch”). See also *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89,93-98 (4th Cir. 2003) (the court concluded that “physical magnetic material on the hard drive is tangible”, but concluded that software and data was not tangible); *Liberty Corp. Capital Ltd. v. Security Safe Outlet, Inc.*, 937 F. Supp.2d 891 (E.D. Ky. Mar. 27, 2013); *Cincinnati Ins. Co. v. Prof’l Data Servs., Inc.*, 2003 U.S. Dist. LEXIS 15859 (D. Kan. July 18, 2003); *AFLAC, Inc. v. Chubb & Sons, Inc.*, 581 S.E.2d 317, 319 (Ga. Ct. App. 2003). But see *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99-185, 2000 U.S. Dist. LEXIS 7299, at 6 (D. Ariz. April 18, 2000) (holding that there was physical damage when information stored on random access memory was destroyed); *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. Minn. 2010) (Insurer had duty to defend lawsuit alleging that a virus caused computer to be unusable, even though the insurance policy excluded “software, data, or other information that is in electronic form” from the definition of “tangible property”); *NMS Servs., Inc. v. The Hartford*, 62 Fed. Appx. 511, 514 (4th Cir. 2003) (*concurring opinion of Judge Widener*); *Centennial Ins. Co. v. Applied Health Care Sys., Inc.*, 710 F.2d 1288 (7th Cir. 1983) (because it was possible that the losses arose from damage to the customer’s tangible property, the duty to defend was triggered); See *Southeast Mental Health*

⁷ The current standard ISO form and other ISO forms since December 1, 2001 specifically exclude “electronic data” from the “property damage” definition. Sometimes endorsements add the coverage back to the policy. It is important to review the insurance policy carefully.

Ctr., Inc., v. Pacific Ins. Co., 439 F.Supp.2d 831, 837-39 (W.D. Tenn. 2006); *Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W. 3d 16, 25 (Tex. App. 2003); *Retail Sys., Inc. v. CNA Ins. Co.*, 469 N.W.2d 735 (Minn. Ct. App. 1991); *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, No. CV97-10380, slip op. at 3-4 (2d Dist. Ct. N.M. May 24, 2000), rev'd in part on other grounds, 46 P.3d 1264 (N.M. Ct. App. 2002).

In first-party property policies, there must be "physical loss or damage" to the covered property for coverage to be triggered. Many first-party property policies contain a broad definition of "Covered Property" that includes all "personal property owned by" the insured. However, software and data may not constitute "personal property" and as such, may not be covered under the policy. Several cases have addressed data losses under first-party property policies. In *Ward General Insurance Services, Inc. v. Employers Fire Insurance Co.*, 114 Cal. App.4th 548 (2003), the insured suffered a computer crash which resulted in a significant loss of electronically stored data. The insurer denied coverage. The court found that the loss did not result in "direct physical loss of or damage to" property and that the data stored on a tangible medium was not tangible. Other courts have found coverage under first-party property policies. See *NMS Servs., Inc. v. The Hartford*, 62 Fed. App'x 511 (4th Cir. 2003) (the court found property damage to hacked computers per a business interruption endorsement); *Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. 2003) (the court found property damage to hacked computers per a business income endorsement); *American Guar. & Liab. Co. v. Ingram Micro, Inc.*, No. 99-185, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. April 18, 2000) (the court found coverage and held that "physical damage" is not restricted to the physical destruction of the computer, but also includes loss of access, loss of use and loss of functionality).

To address court decisions finding coverage under the CGL policies for data breaches, the insurance industry, through the Insurance Services Office ("ISO"), has taken action to remove cyber coverage from CGL policies. In 2013, ISO introduced an *optional* endorsement that deleted the invasion of privacy related offense (oral or written publication, in any manner, of material that violates a person's right of privacy) from the definition of personal and advertising injury applicable under Coverage B of the ISO coverage form.⁸ Thereafter, ISO introduced several other endorsements that further exclude coverage for data breaches. These endorsements have been approved by insurance regulators in 45 states and became effective May 1, 2014. Each of the ISO endorsements broadly excludes data-related losses as well as those arising from the access or disclosure of confidential or personal information of a person or company. The endorsements exclude damages claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred. In

⁸ July 18, 2014 Insurance Journal – ISO Comments on the CGL Endorsements for Data Breach Liability Exclusions.

addition to the exclusions, several insurance carriers have revised the definition of “property damage” in the CGL policies to state:

For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

Companies that suffer a data breach incur significant costs including but not limited to, forensic investigation costs, breach notification costs, credit monitoring costs, crisis management costs, lost business, and legal/litigation costs. To protect themselves, companies can purchase a specialty insurance policy referred to as “Cyber” insurance. Cyber insurance policies can provide coverage for first-party (cyber crime) coverage as well as third-party (cyber liability) coverage. They can provide coverage for direct loss and legal liability with resulting consequential loss caused by cyber security breaches. Cyber insurance policies are usually claims made and can be very expensive, although the costs have come down as more carriers have entered the market. Depending on the policy, there is an ability to insure notification costs, credit monitoring and other direct expenses covered if there is a data breach EVEN if there is never a liability claim. Regulatory fines and penalties are endorsable. Some insurance carriers provide crisis management, a call center, and other services to the policyholder when cyber insurance is purchased. It is important that companies review the policy wording carefully to make sure that it meets their business needs. Some policies are better written than others.

A cyber insurance policy should provide coverage for the following first-party costs⁹:

- Legal and forensic services to determine whether a breach occurred and to assist with regulatory compliance if a breach is verified
- Notification of affected customers and employees
- Electronic information restoration
- Customer credit monitoring and identity protection services
- Crisis management and public relations to educate the company’s customers about the breach;

⁹ See “Department: Technology: Risky Business: Why Lawyers Need to Understand Cyber Insurance for Their Clients”, Shawn Tuma and Katti Smith, 78 Tex. B.J. 854 (December 2015); and “Department: Law Practice Solutions: Everything You Need to Know about Cyber Liability Insurance But Never Knew to Ask”, JoAnn Hathaway, 95 MI B.J. 42 (December 2016).

- Business interruption expenses, such as additional staff, rented or leased equipment, third-party services, and additional labor arising from a coverage claim;
- Public relations firm fees to restore reputation and mitigate damages
- Regulatory fines
- Cyber extortion reimbursement for perils including credible threats to introduce malicious code, pharm and phish customer systems, or corrupt, damage or destroy their computer system.
- Systems failure and administrative error

Similarly, a cyber policy should provide coverage for the following third-party costs¹⁰:

- Judgments, settlements or civil awards
- Electronic media liability, including infringement of copyright, domain name, trade name, service mark or slogan
- Potential employee privacy liability as well as network security and privacy liability

Even companies that purchase cyber liability policies may end up in a coverage dispute with their insurance carriers. *See Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., No. 2:14-CV-170, 2015 U.S. Dist. LEXIS 62185 (D. Utah 2015)* (complaint had to contain allegations of negligence to trigger duty to defend); *Doctors Direct Ins., Inc. v. Bochenek, 38 N.E.3d 116 (Ill.Ct.App. 2015)* (no coverage under cyber claims endorsement for TCPA or consumer protection claims); *Columbia Cas. Co. v. Cottage Health Sys., 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. July 17, 2015)*; and *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. 2016)*.

In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.*,¹¹ the court held that P.F. Chang's cyber liability policy did not provide coverage for over \$1.9 million in fees and assessments that P.F. Chang's was required to pay Bank of America Merchant Services ("BAMS"). BAMS had provided P.F. Chang's with credit card processing services. Under the Master Services Agreement ("contract") between P.F. Chang's and BAMS, P.F. Chang's was required to reimburse BAMS for fees, fines, penalties or assessments BAMS paid to MasterCard. After hackers stole the credit card data of approximately 60,000 of P.F. Chang's customers, BAMS paid over \$1.9 million in assessments to MasterCard and sought reimbursement of those costs from P.F. Chang's per the contract. The cyber policy issued by Federal Insurance

¹⁰ *Id.*

¹¹ *No. CV-15-01322-PHX-SMM, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. 2016)*

Company had a narrow definition of “privacy injury” and contained an exclusion for any loss or expense that P.F. Chang’s assumed under a contract.

The policy at question in *P.F. Chang’s* was marketed by the insurer as “a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today’s technology-dependent world” covering “direct loss, legal liability, and consequential loss resulting from cyber security breaches.”¹² But the policy language was more particular and, ultimately, determined by the district court to be less expansive in the coverage afforded. The insuring agreement in the policy stated that the insurer shall be liable for loss on account of claims made against the insured for covered injury, including a “Privacy Injury,” defined as an “injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person’s Record”¹³ Federal’s cyber policy also contained an exclusion for any loss or expense that P.F. Chang’s assumed under a contract.¹⁴ Federal argued that there was no coverage under the insuring agreement for the \$1.9 million in assessments and fees and that in any event coverage was barred under the exclusion for liabilities assumed under contract. As to the insuring agreement, Federal argued that the data breach did not constitute a “Privacy Injury” since the “Records” compromised were not the records of BAMS, the card-processing entity that had presented the \$1.9 million assessment claim to P.F. Chang’s.¹⁵ P.F. Chang’s argued that a “Privacy Injury” existed regardless of who suffered it.¹⁶ The policy language would seem to support the P.F. Chang’s position on this point since, even with a close parsing of the definition of “Privacy Injury,” the policy does not expressly require a covered “Privacy Injury” to have been sustained by the entity asserting the claim against the insured for such injury, and the definitions of “Person” and “Claim” do not support any such restriction.¹⁷ The court assumed, without discussion, that the injury must be an injury suffered by the entity presenting the claim, and held that there was no coverage for the assessment under the insuring agreement because “BAMS did not sustain a Privacy Injury itself, and therefore cannot maintain a valid Claim for Injury against Chang’s.”¹⁸ The court further held that coverage for the assessment was barred by the policy exclusion for contractual obligations arising between the insured and a third party, BAMS.¹⁹

¹² 2016 WL 3055111, at *1.

¹³ *Id.* at 4. The capitalized terms are terms defined in the policy.

¹⁴ *Id.* at 7.

¹⁵ *Id.* at 5.

¹⁶ *Id.*

¹⁷ Def. Fed. Ins. Co’s Answer and Affirmative Defenses to Pl’s Compl. for Breach of Contract and Declaratory J., Ex. 1 at 2, *P.F. Chang’s China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016).

¹⁸ 2016 WL 3055111 at 4.

¹⁹ *Id.* at 7.

P.F. Chang's relied upon the reasonable expectation doctrine in its further argument that the court should interpret the policy language to find coverage for the card-processing assessments for the data breach, presenting evidence of the insurer's marketing representation that the policy addressed "the full breadth of risks associated with doing business in today's technology-dependent world"²⁰ and that it would cover direct and "consequential loss resulting from cyber security breaches" and deposition testimony of Federal's underwriter showing that, at the time the policy was renewed, Federal knew that all of the credit card transactions done by P.F. Chang's were processed through a servicer like BAMS and knew that P.F. Chang's would have liability for the type of assessment at issue in this case in the event of a data breach regarding credit card transactions.²¹ Nonetheless, the court declined to apply the reasonable expectation doctrine, stating that regardless of Federal's understanding, "[n]owhere in the record is the Court able to find supporting evidence that during the underwriting process Chang's expected that coverage would exist for Assessments following a hypothetical data breach."²² The court considered P.F. Chang's to be a sophisticated insured and commented, "[I]f Chang's, who is a sophisticated party, wanted coverage for this Assessment, it could have bargained for that coverage."²³

Some cyber policies now explicitly provide coverage for the type of assessment that the Arizona court found not to be covered by the cyber policy at issue in *P.F. Chang's*, referred to as Payment Card Industry (PCI) coverage. This PCI coverage explicitly covers the assessments made by credit card issuers due to a data breach. Policies providing explicit PCI coverage may contain an affirmative insuring agreement covering contractually imposed PCI-DSS fines, penalties and assessments and an exception to the standard contractual liability exclusion.²⁴ Nevertheless, the decision in *P.F. Chang's* provides important lessons for policyholders possessing or dealing with private or sensitive data vulnerable to security breach. For one, the court in *P.F. Chang's* found that the insured's alleged expectation regarding its policy coverage was a "*non sequitur*" from the marketing statements and other evidence the insured had presented, which conclusion was unsupported by any evidence or proof as to what its *actual expectations* were.²⁵ Policyholders hoping to recover for cyber breaches under the reasonable expectation doctrine must therefore be able to provide an affirmative showing of such expectations. This could be done through deposition testimony with explicit statements of the

²⁰ *Id.* at 1.

²¹ *Id.* at 9.

²² *Id.*

²³ *Id.* at 5.

²⁴ Integro Insurance Brokers, Insurance Broking & Consulting White Papers, *Learning A Lesson From P.F. Chang's*, available at <http://integrogroupp.com/news/integro-white-papers/learning-a-lesson-from-p.f.-changs>

²⁵ *P.F. Chang's*, 2016 WL 3055111, at *9.

insured's representatives on expected coverage²⁶ or other demonstrations of anticipated risks and coverage.²⁷ *P.F. Chang's* also highlights an important issue that may recur in determining coverage claims under cyber policies, which is whether a "privacy injury" covered by a particular policy has to be an injury sustained by the claimant. In *P.F. Chang's*, the Court rejected the insured's argument that "privacy injury" is to be construed broadly to also cover those sustained by the credit card issuer imposing the assessments for breach of its credit card information, as the claimant (BAMS) was merely acting as a pass-through intermediary.²⁸ Under the insured's reasoning, an intermediary such as BAMS is not the true injured party, and will likely never be. Would the court's interpretation of "privacy injury" in this context then preclude coverage for all claims presented by intermediaries?

How Can Companies Make Sure That Their Cyber Policies Provide Coverage for Data Breaches?

Companies should develop and maintain a risk management program for addressing their cybersecurity risks. Besides knowing the federal, state, and local laws and regulations, companies should thoroughly assess their own cybersecurity risks through a risk assessment. The assessment should include:

- Defining the system
- Identifying and classifying critical cyber assets
- Identifying and documenting the electronic security perimeters
- Performing a vulnerability assessment
- Assessing risks to system information and assets

²⁶ *State Farm Fire & Cas. Co. v. Rocky Sapp, No. 1 CA-CV 13-0623, 2015 WL 632138, at *1-6 (Ariz. Ct. App. Feb. 12, 2015), review denied (July 30, 2015)* (Policyholder, through his testimony, demonstrated that he believed he had the requisite coverage, stating that "he would not have purchased the...policy had he known that coverage would not be extended" accordingly.)

²⁷ See, e.g., *Hawkins v. Globe Life Ins. Co.*, 105 F. Supp. 3d 430, 442-44 (D.N.J. 2015) (Although insurer argues that its solicitation materials specifically stated coverage was not effective until approved by the company, policyholder reasonably expected coverage in the interim period at issue because insurer received the policyholder's premium check and cashed the check); *Haber v. St. Paul Guardian Ins. Co.*, 137 F.3d 691, 697-98 (2d Cir. 1998) ("When an individual notifies an insurer of its desire to obtain full coverage and of the existence of a live-in housekeeper, a court may infer an intention on the part of the individual to cover the employee. This inference, coupled with the complete reading of the Endorsement in question, could certainly lead an average person to reasonable expect that he has the coverage sought."); *Meadow Brook, LLP v. First Am. Title Ins. Co.*, 2014 MT 190, ¶ 17, 375 Mont. 509, 514, 329 P.3d 608, 612 (In addition to email correspondence between policyholder and insurer discussing a request for an endorsement, policyholder paid significant money for an endorsement to the title policy for additional coverage).

²⁸ 2016 WL 3055111, at *5.

- Selecting security controls
- Monitoring and assessing the effectiveness of controls using pre-defined metrics
- Developing and implementing effective cybersecurity policies
- Determining the level of understanding of employees with respect to cybersecurity and whether training is needed

Attached is a chart setting forth a gap analysis of cyber insurance coverage, as well as the Willis Towers Watson Winter 2016 Cyber Claims Brief. Recently, the American Bar Association Cybersecurity Legal Task Force created a Cybersecurity Checklist.²⁹

Conclusion

Cyber breaches can be risky for businesses. A good risk management plan, along with appropriate insurance, can help businesses successfully maneuver coverage obstacles in the event of a cyber breach. Cyber policies³⁰, commercial property policies and CGL policies are just a few of the sources of coverage to evaluate. Depending upon the circumstances, policyholders should also review their crime policies³¹, directors & officers' liability policies and their errors and omissions or professional liability policies. Some insurance policies may not include exclusions and other language to limit coverage for cyber breaches. Should a cyber-breach occur, it is worth reviewing various policies carefully to see what coverage, if any, may be available.

²⁹ See

http://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf

³⁰ Cyber extortion policies are also available on the market.

³¹ See *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821 (6th Cir. 2012), where the claim was submitted under a computer fraud rider to a Blanket Crime Policy and the court found that the data breach loss "resulted directly from the hacking, and an exclusion for loss of confidential information did not apply to the loss of customer information; *Medidata Solutions, Inc. v. Fed. Ins. Co.*, Civ. Action, 2016 U.S. Dist. LEXIS 178501 (S.D.N.Y. 2016); *Bitpay, Inc. v. Mass. Bay Ins. Co.*, Case No. 1:15-cv-03238 (N.D. Ga. Mar. 17, 2016) (Order attached); *Ameriforge Group, Inc. v. Fed. Ins. Co.*, Case No. 4:16-cv-00377 (S.D. Tex. 2016); *Principle Solutions Group, LLC v. Ironshore Indem., Inc.*, Case No. 1:15-cv-04130 (N.D. Ga. Aug. 30, 2016) (Order attached); and *Taylor & Lieberman v. Fed. Ins. Co.*, 2015 U.S. Dist. LEXIS 7935 (C.D. Cal. 2015).

Cyber Liability: GAP Analysis example

1 st Party Privacy/Network Risks	Property	General Liability	FI Bond & Crime	Proposed Privacy/Cyber
Physical damage to Data	Likely Covered	X	Likely Covered	Covered
Virus/Hacker damage to Data	Likely Covered	X	Likely Covered	Covered
Denial of Service attack	X	X	X	Covered
B.I. Loss from security event	X	X	X	Covered
Extortion or Threat	X	X	X	Covered
Employee sabotage	X	X	Limited	Covered
3 rd Party Privacy/Network Risks				
Theft/disclosure of private info	X	X	X	Covered
Confidential Corporate Info breach	X	X	X	Covered
Technology E&O	X	X	X	Covered
Media Liability (electronic content)	X	Limited	X	Covered
Privacy breach expense/notification	X	X	X	Covered
Damage to 3 rd party's data	X	X	X	Covered
Regulatory Privacy Defense/Fines	X	X	X	Covered
Virus/malicious code transmission	X	X	X	Covered



Cyber Claims Brief

Winter 2016

A semi-annual publication from the FINEX Claims & Legal Group

Editors

Adeola I. Adele

Cyber Thought Leader

adeola.adele@willistowerswatson.com

Brian Weiss

Claim Advocate

Regional Team Leader

brian.weiss@willistowerswatson.com

Dan Twersky

Claim Advocate

dan.twersky@willistowerswatson.com

Contributors

Tom Brown

Global Leader

Cyber Security & Investigations

Berkeley Research Group, LLC

tbrown@thinkbrg.com

Jim Devoe

Cyber Coverage Analyst

jim.devoe@willistowerswatson.com

Emily Lowe

Cyber Broker

emily.lowe@willistowerswatson.com

Gina Macari

Claim Advocate

gina.macari@willistowerswatson.com

David Navetta, Esq.

Partner

Norton Rose Fulbright US LLP

david.navetta@nortonrosefulbright.com

Matthew Spohn, Esq.

Senior Counsel

Norton Rose Fulbright US LLP

matthew.spohn@nortonrosefulbright.com

I am particularly excited to present the Winter 2016 edition of Willis Towers Watson's Cyber Claims Brief. This edition is the first of its kind from the insurance brokerage industry in that it centers on a set of data collected from the cyber claims we've reported to insurers during the last five years on behalf of our clients ("the Willis Towers Watson "Reported Claims Index").¹ We have incorporated within each article specific findings from the Reported Claims Index in order to provide additional, thought-provoking insight into some of the key trends of 2016, and what we expect to see develop in the coming year.

While much has previously been written in the privacy and security world about the dangers posed by hackers and the potential damages unauthorized network intrusions can cause, Emily Lowe and Berkeley Research Group's Tom Brown take a closer look at the hackers themselves; specifically, who they are, what motivates them to carry out attacks and what they're likely to do with the digital assets they've stolen.

Combining our Reported Claims Index with some of the results from a cyberrisk survey we commissioned this past summer to better understand organizations' cyberrisk management priorities, Brian Weiss highlights the link between security awareness training for employees and the potential impact on frequency of employee-related cyberincidents.

As organizations continue to outsource various aspects of their businesses, the number of cyberincidents originating from third-party vendors continues to increase. Adeola Adele, in collaboration with Norton Rose Fulbright's David Navetta and Matthew Spohn, discuss the increase in third-party-related breaches, answer some frequently asked questions regarding the respective responsibilities of the involved parties following a breach, and provide key considerations for drafting vendor contracts, as well as additional insured coverage under cyberinsurance policies.

As regulatory enforcement is ramping up, especially in the health care sector, Gina Macari hones in on some of the largest HIPAA settlements, claim trends and provides recommendations regarding insurance coverage for HIPAA fines and penalties.

Finally, recognizing that Network Business Interruption incidents are on the rise, Jim Devoe and Dan Twersky take on one of the most noteworthy cybercase studies of 2016, and opine on how a typical cyberinsurance policy might respond.

We hope you enjoy this edition and, as always, we look forward to your comments and feedback.

Kenneth Ross

Executive Vice President, Willis Americas Administration, Inc.

Director, FINEX Claims & Legal Group and Thought & Product Leadership

+1 212 915 8083

ken.ross@willistowerswatson.com

¹ The Reported Claims Index is a collection of representative cyber claims of all different incidents, severity, and loss amounts we have selected for inclusion in our claims study mentioned throughout this edition of the Cyber Claims Brief, and to be incorporated into future editions.

Know your enemy

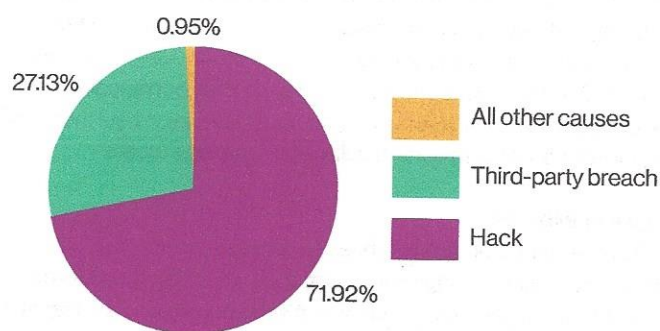
Inside the hacker's mind

By Tom Brown with Emily Lowe

Companies rely on technology and outsourcing for critical activities, including storing sensitive client data and intellectual property, communicating and conducting transactions. This leaves them vulnerable to cyberattacks. Whether from company insiders or outside hackers, these attacks can interrupt business operations, result in the theft of proprietary information, or cause the loss of customers' data — with devastating effects on a company's reputation and bottom line. The threat of litigation and increased regulatory scrutiny have broadened this risk and escalated potential losses.

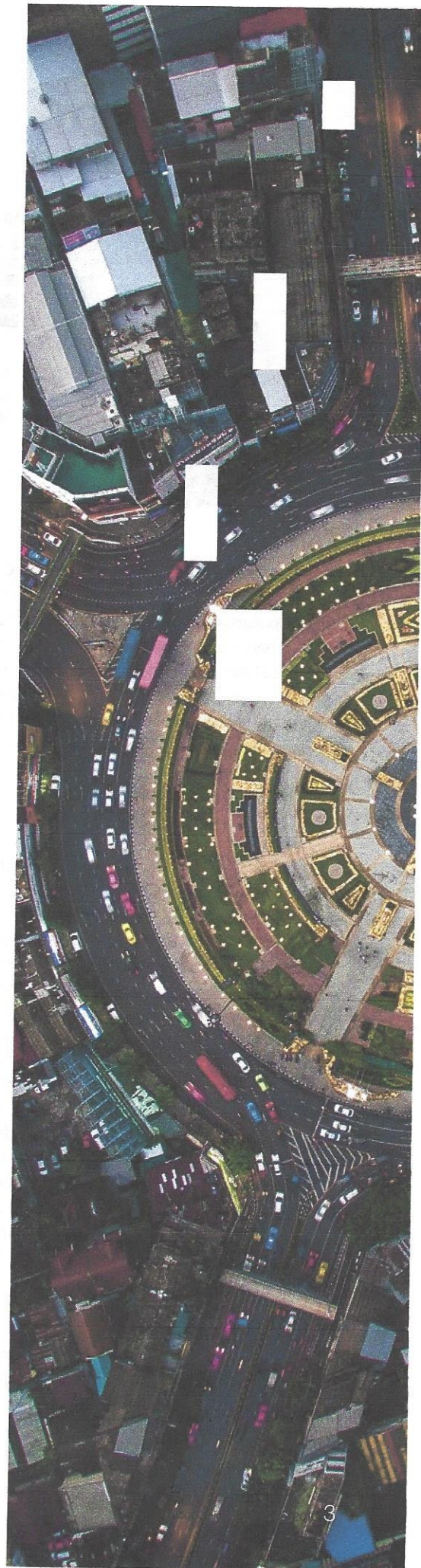
The below charts created from the Willis Towers Watson Reported Claims Index highlight that organizations need to remain vigilant against threats to their network and information assets. While many organizations experience daily attacks on their networks, events causing significant damage appear to be uncommon. However, the results from our data suggests that when an attack does succeed, it impacts a disproportionately larger amount of personally identifiable information (PII), which has a greater overall financial impact than other claim categories. While hacking incidents accounted for only 17.28% of the incidents within the Reported Claims Index, they represented 71.9% of the total records compromised. Therefore, as organizations consider how best to protect themselves with technology, tools and procedures, those efforts may be less effective if organizations do not understand who is behind cyberattacks, how the attackers operate and what motivates them.

Records lost by breach type

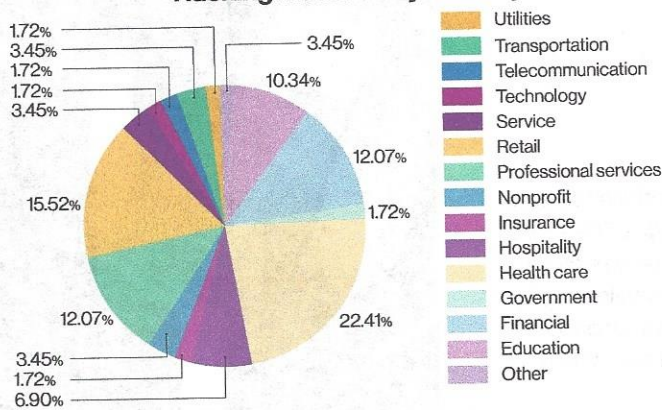


Average number of records lost by type of breach

Hack	1,979,820.61
Third-Party Breach	1,332,479.91
Lost/Stolen Device	5984.114
Rogue Employee	4570.225
Accidental Disclosure	3551.856
Social Engineering	19.25
Other	16.333



Hacking incidents by industry



Who are the hackers? What drives them?

While reports of data breaches at the largest retailers, banks, health care companies and Internet service providers often appear in the news, the hackers behind these cyberattacks are not as well known. Experience teaches that there are at least four broad categories of attackers: financially motivated cybercriminals, “hacktivists,” nation-state-supported actors, and malicious insiders. We often see overlapping motivations among the attackers.

Financially motivated cybercriminals

The driving force behind financially motivated attackers is clear: to steal and monetize information or hold systems hostage to extort ransom payments. This threat is illustrated by a case that was brought by United States federal authorities against an international cybersyndicate based in Russia and Estonia that targeted U.S. financial institutions. Members of the criminal organization had specialized, interlocking skills and tasks that combined to ensure the success of the conspiracy. One set of conspirators broke into an ATM processing network and stole online banking credentials for hundreds of thousands of bank customers. Another set recruited and directed “mules,” accomplices who in turn encoded blank plastic cards with the stolen information and used them to withdraw millions of dollars in cash from ATMs all over the world. Still other conspirators laundered the proceeds, including by converting it into WebMoney, a digital currency popular in the former Soviet bloc that is easily transmitted online and as anonymous as cash. Two conspirators arrested in New York City, both Ukrainian nationals living in the U.S. illegally, were alone found to have fraudulently withdrawn over \$2 million from ATMs in just a matter of weeks using stolen account information that they had received from a co-conspirator in Russia.

“Hacktivists”

So-called “hacktivists” are cybercriminals who purport to commit cyberattacks in support of an ideology. A well-known example of hacktivism is the sprawling, loosely organized online group known as

“Anonymous.” Although many who identify with Anonymous don’t commit crimes to advance their agenda, there are others who do. One such sub-group of criminal hackers was known as “LulzSec.” Its members used encrypted, invitation-only online chatrooms to plan attacks and an eponymous website and Twitter account to spread propaganda, seek monetary support in the form of Bitcoin donations, taunt victims and dump stolen information online. United States federal prosecutors charged the core leadership of LulzSec, which comprised individuals living in the United States, the United Kingdom and Ireland and who ranged in age from their late teens to mid-twenties, with a variety of hacking offenses. LulzSec’s leaders and their co-conspirators broke into computer systems used by several media companies and government entities, among hundreds of other victims in the education, financial services, travel and entertainment, technology, media, health care and consumer products sectors. These hacks resulted in the theft and disclosure of PII of over one million victims, not to mention the remediation costs suffered by the organizations whose computer networks were compromised.

Nation state actors

Nation state actors can be classed as foreign government agents or cybercriminals working on their behalf and whose agenda can range from stealing economic information to launching disruptive or destructive attacks. In the case of the *United States v. Wang Dong, et al.*, federal authorities charged five members of the Chinese military with hacking into computer systems owned by six American victims in the U.S. nuclear power, metals and solar products industries with the purpose of stealing information useful to competitors in China, including state-owned enterprises. In the *United States v. Amad Fathi et al.*, seven hackers who were sponsored by the Iranian government were charged with disabling the websites of 46 major companies in the United States, primarily in the financial sector, which cost the victim organizations tens of millions of dollars in remediation costs.

Rogue employees

Malicious insiders, often disgruntled employees, seek to take advantage of their privileged access to steal valuable information or disrupt or destroy computer systems. A scheme involving a trader at a large bank illustrates this type of attacker. Recruited by a competitor to build a high-frequency securities trading platform, the employee, who was unable to do the work on his own, stole the necessary computer code worth millions of dollars from his employer. Indeed, rather than use any sophisticated means of attack, the employee took advantage of his insider status simply to print out the computer code on hundreds of sheets of paper, which he took home and analyzed. Charged with economic espionage, the employee was found guilty in federal court following a two-week trial.

How do hackers infiltrate victim computer networks?

The means by which outside attackers gain unauthorized access to computer systems varies widely, from the low-tech to the most sophisticated manipulations. Simple attacks, like phishing emails which carry a malware payload, are often surprisingly effective and can permit a hacker deep access to a target network. On the other end of the scale are hacks which rely on the exploitation of known, but unpatched vulnerabilities in computer systems, or even so-called "zero days," undetected flaws that are known only to the attacker. A basic rule of thumb is that no matter the means, a determined hacker will eventually be successful. Time is on the attacker's side, whereas a computer network administrator needs to prevent attacks 100% of the time.

How can clients lower the likelihood of a hack?

There is no one-size-fits-all approach to cybersecurity — every organization is different. There are, however, some basic elements that companies may wish to consider as a means of reducing their cyberrisk. A starting point is the development and implementation of a comprehensive information security plan. Once applied, such a plan should be reviewed and updated regularly in light of the often dynamic nature of computer networks and the threat environment. A comprehensive information security plan may include, among other things, a cyberrisk assessment, involving external penetration testing (sometimes called ethical hacking, in which external cyberdefenses are tested), as well as an internal evaluation. For example, are software patches applied in a timely fashion? Is the network adequately segmented? Are network logs appropriately detailed and maintained?

The two questions above are commonly asked by insurers on applications for cyberinsurance. The latter question may be especially relevant to investigating a hack. Logs may provide valuable forensic data, potentially permitting an investigator to look back and determine how a hack occurred, whether a system is still compromised, and what data, if any, was exfiltrated. In addition, a comprehensive information security plan may also include an incident response blueprint. Speed is often important in dealing with a cyberattack, and a "break glass" incidence response plan may increase the efficiency of a response and help with the preservation of data important to a forensic assessment. Finally, organizations may wish to consider their culture of security. Engagement by senior management coupled with regular training, which raises awareness among employees, may help defend against low-tech attacks like phishing emails and promote an overall emphasis on cyberdefense.

Taking these steps will help prevent or reduce the frequency of hacking claims and the associated financial loss and reputation damage.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group, LLC or its other employees and affiliates.

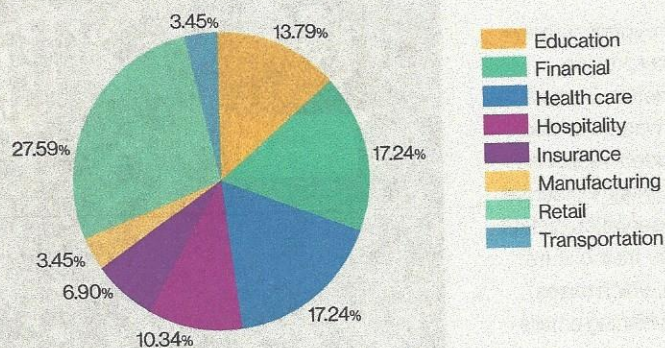
Tom Brown is Global Leader of Berkeley Research Group's Cyber Security/Investigations practice. He specializes in helping clients manage cyberrisk, respond to incidents, remediate vulnerabilities, and address post-incident regulatory inquiries and litigation. Prior to joining BRG, Tom served for 12 years as an Assistant United States Attorney in the U.S. Attorney's Office in Manhattan, where he supervised the Complex Frauds and Cyber Crime Unit. He led some of the most technologically challenging cases ever pursued by the U.S. government, including successful investigations of the underground drug website Silk Road and the hacktivist group Anonymous. Tom is a recipient of the FBI Director's Award for Outstanding Cyber Investigation and was named "Prosecutor of the Year" by the Federal Law Enforcement Foundation in 2011. He is a member of the New York bar. Tom is based in New York.

More vendors, more problems

By Adeola Adele, David Navetta, Esq. and Matthew Spohn, Esq.

The reliance on third-party vendors, whether directly or indirectly, has increased dramatically with technological advancements and competition. At the same time, several studies have reported that loss or compromise of data in the hands of such third-party vendors accounts for a significant percentage of all data breaches or cyberattacks. For example, according to the Ponemon Institute report of May 2016, 75% of the IT and security professionals surveyed stated that the risk of a third party's breach is a serious concern and increasing within their organizations. This view appears to be supported by Willis Towers Watson's data which indicates that of the Reported Claims Index, data held by third parties accounted for 27% of the total 112,890,290 lost or otherwise compromised records involved in those claims

Third party breaches by industry



As shown on the above chart, third-party cyberincidents were more prevalent in the retail, financial services and health care industries.

Notably, the cost on the black market of stolen financial and health care records — records likely to be controlled by a vendor — is far greater than that of other stolen records given the value of such information, including their use in social engineering schemes and other criminal acts. One recent study found that a breach involving medical records, customer financial records or credit cards will cost a company an average of \$7 million in 2016, when lost customers are factored. Analyzed in another way, the cost averaged \$221 for each lost or stolen record. (See <https://securityintelligence.com/media/2016-cost-data-breach-study/>). Given the potential costs associated with loss/disclosure of customer data, below are some of the questions that companies ask when negotiating vendor contracts:

If my vendor is breached that's the vendor's problem, right?

Unless a contract states otherwise, it is almost always true that an organization has ultimate responsibility for breach of its data while in the hands of a vendor. According to data breach statutes enacted in the majority of states, the owner of the personal data — not the vendor who is handling it — has the primary obligation to investigate the breach and provide any required notice to the affected individuals. The same is true with respect to medical information protected by federal and state laws.

Accordingly, if the organization's sensitive data is breached while under the control of a vendor, the vendor's primary obligation is to notify the organization. It is then the customer's obligation to handle the fallout, unless the customer's contract with the vendor provides otherwise.

My vendor warrants that it will keep my information confidential, won't that protect me?

Even where the vendor unequivocally warrants that it will keep the customer's data confidential, there is the question of the remedy for breach of that warranty. The typical vendor contract contains a section titled "limitation of liability" with two key provisions: one capping the vendor's total liability (often the total fees paid under the contract, or fees paid in the prior 12 months), and another stating that in no event will the vendor be liable for any consequential, incidental, or indirect damages (typically known as a "consequential damages waiver").

The damages cap is straightforward: even for a breach of the contract, the customer cannot recover more than that cap from the vendor. Careful consideration should be given to whether that cap adequately protects the company in the event of a data breach.

But organizations must also pay close attention to the consequential damages waiver. The law generally defines consequential damages as those damages that are not foreseeable to a stranger to the contract, but are foreseeable to the parties to a contract at the time they signed it, given what they know of the transaction. But even judges will admit that this definition is difficult to apply in practice. The result is that in the case of a data breach, one could argue that some or all of the resulting damages — costs to notify affected individuals, costs to respond to regulators' investigations, etc. — are

consequential damages. If that is correct, then a consequential damage waiver will bar any recovery of those damages. As a result, customers need to pay particular attention to any consequential damages waiver in a vendor contract.

My vendor contract has an indemnity clause, won't that protect me?

In addition to warranties and damages limitations, most vendor contracts will contain some sort of indemnity provision. For instance, a basic indemnity provision would require the vendor to "defend and indemnify Customer against any third-party claim, suit, or proceeding arising out of Vendor's material breach of this Agreement." Such indemnity clauses are often carved out from the contract's damages cap and consequential damages waiver. However, standing alone, they may not provide adequate protection against data breaches.

The primary limitation of a standard indemnity clause is that it may only cover lawsuits brought against the customer as a result of the data breach (assuming the contract is drafted so that the data breach qualifies as a breach of the agreement). Such third-party claims, though, are a relatively rare consequence of a data breach. Where millions of customer records are breached, one can expect a class action lawsuit brought on behalf of the affected individuals. Data breaches with less than 100,000 affected individuals are less likely to interest a plaintiff's lawyer, who typically is only paid a percentage of the final recovery.

In such cases, the more likely consequences are the costs to comply with the relevant data breach notification statutes and to address the public relations issues. These include the costs of hiring forensic investigators to assess and remediate the breach; attorneys' fees to determine the legal obligations triggered by the breach, and to respond to any investigation by state regulators or law enforcement; costs of identifying affected individuals and sending the required notices; costs to set up and staff call centers; costs of credit monitoring services that may be offered to affected individuals; and potential regulatory fines and penalties imposed by state agencies. An indemnity clause can be drafted to shift responsibility for all these costs to the vendor in the event of a data breach, but such language is unlikely to be found in the vendor's standard contract.

Will a well-drafted vendor contract fully protect me?

The best contract is only so good as the other side's willingness or ability to perform. Where there is a claim for breach or indemnity, the other side may be motivated to fight the claim in litigation. Such litigation can be expensive and time-consuming. Even if the vendor contract provides that the loser pays the winner's attorneys' fees, recovery can be delayed by the litigation and appeals process. At the end of that litigation (or even if there is no litigation at all), there

is always the question of collectability — does the vendor have sufficient assets to satisfy a judgment? If not, then the organization's contractual protections could be rendered virtually worthless.

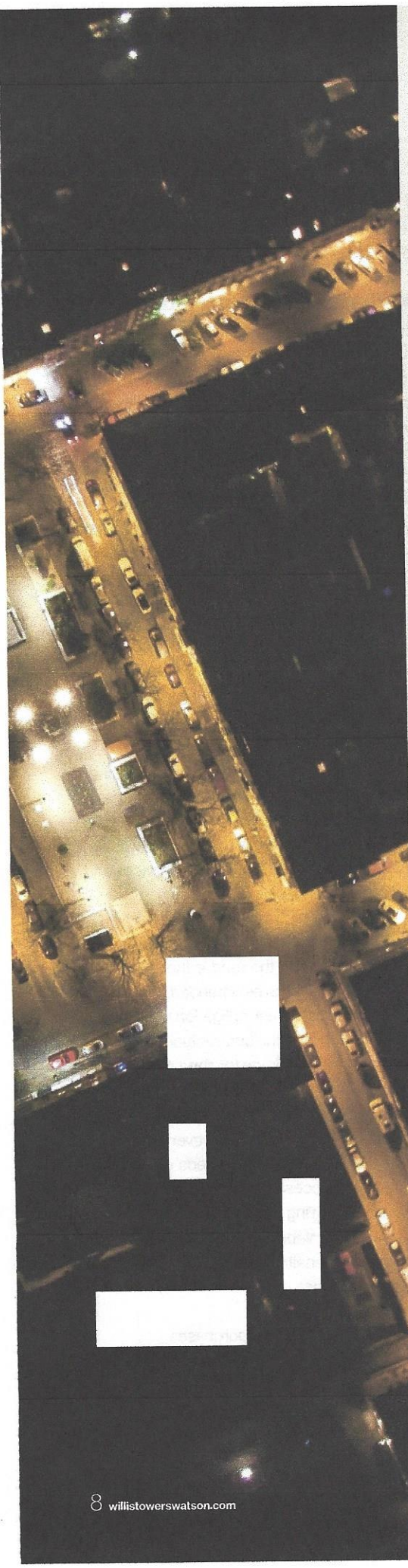
What if I have the vendor add me as a named insured on its cyberinsurance policy?

Cyberinsurance policies are intended, among other coverages, to protect loss or disclosure of the insured's data, and they can provide additional protection against third-party data breaches. When the insured vendor has agreed to indemnify its customer for loss or disclosure of the customer's data, the vendor may want to amend its insurance policy to include the customer as an "additional insured." The customer may want this as well, as it can help protect against any claims brought against the customer due to the vendor's wrongful acts or errors.

However, the scope of coverage would depend on the type of services the vendor has agreed to provide to its customer. For example, where the vendor's services include direct access to the customer's network or when the vendor holds the customer's confidential data, the vendor's technology errors and omissions policy should include network security and privacy coverage. In this case, the coverage can be written to include loss, disclosure and theft of data in any form, as well as network security failure, denial of service attacks, and transmission of malicious code. If agreed by contract, the coverage can also be negotiated to include some first-party costs such as: data breach regulatory fines and penalties, the cost of notifying individuals of a security or data breach, the cost of credit monitoring services and any other related crisis management expense.

If a customer is named as an additional insured, then to allow coverage for a claim brought by the customer against the vendor, the policy's Insured v. Insured exclusion may also need to be amended. If it is not, the insurer could invoke it to avoid covering any obligation that the vendor may have to its customer. Similarly, the contractual liability exclusion — which typically precludes coverage for any liability the insured assumed under a contract — may need to be deleted or amended to provide an exception for the vendor's contractual indemnification of its customer. This amendment, however, is more difficult to achieve as most insurers consider the insureds' contractual obligation to be pre-existing and not necessarily one that flows from the cyberincident. As such, after reviewing the vendor contract, insurers will typically only provide a carveback for certain losses (such as Payment Card Industry fines and penalties) rather than all damages contemplated under the vendor contract.

Additional issues are raised if the customer also purchases cyberinsurance and the vendor has agreed to provide "additional insured" coverage. In that case, the customer should consider



amending the "other insurance" clause of its own cyberinsurance policy to ensure that the vendor's policy would apply as primary insurance in the case of a breach caused directly or indirectly by the vendor. It is worth noting that unless the policy is otherwise endorsed, the vendor and its insurer may then have full control of the claim, including selection of breach counsel, forensic investigators, public relations and any other first-party loss protection offered under the policy.

Ultimately, the goal of the "additional insured" coverage afforded to the customer is to ensure that coverage is being provided only for claims arising from the vendor's wrongful acts or errors, whether directly or indirectly (rather than the acts or errors not within the vendor's control). Providing insurance coverage to the customer beyond that which is contractually or legally required could unintentionally limit the coverage available to the vendor for its own wrongful acts.

Conclusion

There is no "one size fits all" protection against the risks presented when vendors have access to customers' data. Those risks are best addressed in consultation with attorneys, insurance advisors and brokers, and any in-house security or IT personnel. Some of the topics to be discussed with those advisors include:

- What are the risks inherent in the types of data that the vendor will have access to? Does it include Social Security numbers, medical information, credit card information or other data subject to state data breach laws? Does it include other information that is not subject to those laws, but could cause harm or embarrassment if disclosed?
- Is there a way to limit the data to which the vendor has access? If not, can it be encrypted to lessen the risks of breach, or can other prophylactic security measures be employed?
- What are the potential costs and consequences in the event the company's data is breached in the hands of the vendor, and how can the vendor's contract properly allocate those risks? If the vendor refuses to accept the proposed terms, are there other ways that the risks can be addressed? If not, does the company need to look at other vendors?
- Consider working with an attorney to create your own template for your company's vendor contracts, with robust terms addressing the company's rights and remedies in the event of a data breach. Many vendors will agree to at least start with the customer's template when negotiating an agreement. However, counsel should still be consulted when vendors attempt to negotiate changes to the agreement, and especially those provisions addressing confidentiality, warranty, indemnification and limitation of liability.
- Prevention is the best medicine: due diligence on a vendor's data security protocols may help identify vendors who present a higher risk of a breach, and investigation into a vendor's finances may help determine whether the vendor can satisfy its obligations in the event of a breach.
- The role of insurance: when carefully crafted, insurance can help mitigate the costs associated with loss of customer data but, to the extent possible, it must be aligned with the obligations assumed or transferred under the vendor contract.

Willis Towers Watson has arranged for Norton Rose Fulbright US LLP to offer its clients a unique service starting in January 2017. For a special flat fee per contract, Norton Rose Fulbright will analyze companies' contracts with their vendors and rate the contracts terms addressing cybersecurity and privacy risks. Clients will receive a report explaining contract's strengths and weaknesses, and identifying areas of risk. Contact Jason Krauss, Cyber & E&O Product Leader at 212-915-8374 or jason.krauss@willistowerswatson.com for more information.

The human element of cyberrisk

Why it pays to sweat the small stuff

By Brian Weiss

This summer Willis Towers Watson commissioned a survey of 306 risk, finance, human resources, information technology and operations decision makers to gain insight into their organizations' cyberrisk priorities. Of those surveyed, 64% indicated that human capital and employee solutions are a very important focus for cyberloss control, and 36% indicated they are a somewhat important focus. Looking at a longer horizon, 68% viewed human capital and employee solutions (which includes cybersecurity awareness training) as a very important future focus for their organizations.

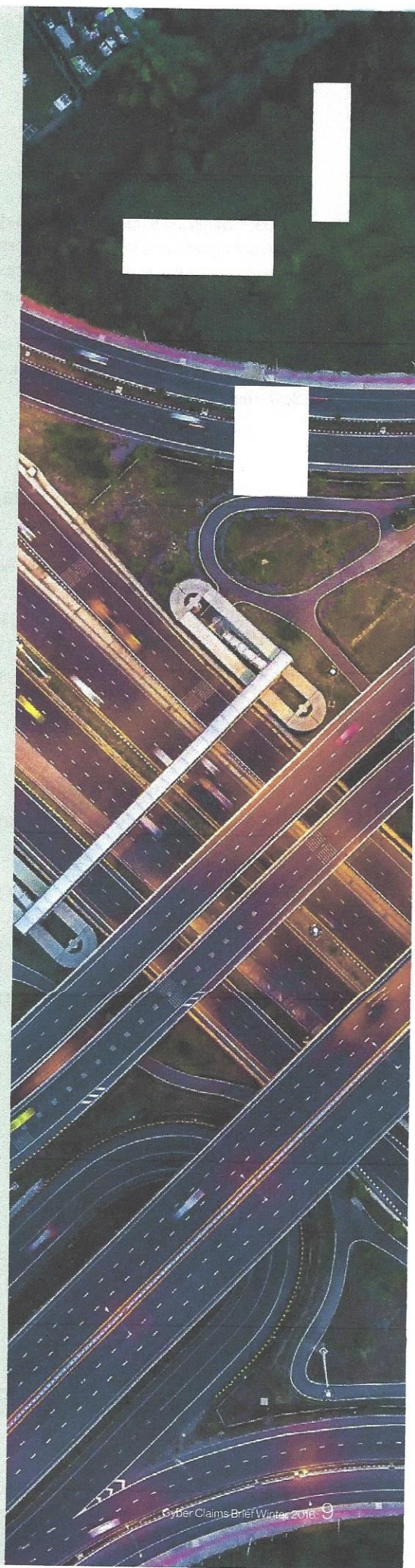
Interestingly, those we surveyed with roles in information technology and operations were more focused on employee solutions than the other interview groups. Both groups had over 70% of participants viewing employee-related cyberrisk as very important. Conversely, of those surveyed in risk and finance, only 55% deemed human capital and employee solutions as a current very important focus. The results highlight the need for organizations to focus more attention and resources to cyberrisk created by employees and their role in overall cyberrisk mitigation.

In the Summer 2016 edition of the Cyber Claims Brief we noted that employees are the first line of defense for companies. We described the risk created by employees and how IOT (the internet of things), BYOD (bring your own device) policies, and the changing face of the workforce combined to accelerate that risk. The Willis Towers Watson Reported Claims Index provides additional support for this reality — the number of cyberincidents involving lost data by the negligence of employees far exceeds the number of incidents caused by bad actors.

Percentage of Claims By Breach Type

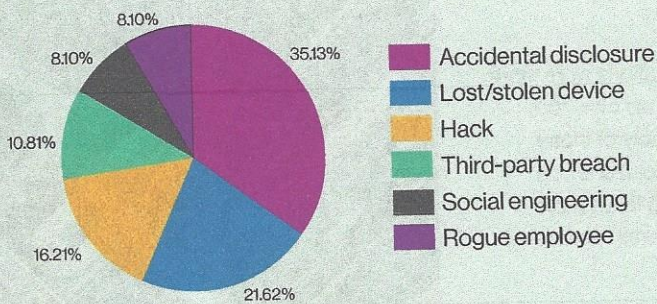
Accidental Disclosure	32.72%
Lost/Stolen Devices	21.43%
Hack	17.28%
Rogue Employee	11.52%
Third-party Breach	7.6%
Social Engineering	3%
Network Business Interruption	2.07%
Other	7.13%

Approximately one-third (32.7%) of all cyberincidents in the Willis Towers Watson Reported Claims Index are caused by accidental disclosures, with lost (or stolen) devices accounting for another 21% of incidents. This trend was most pronounced in the health care industry, where almost half of our clients' cyberincidents can be attributed to accidental disclosures, and another one-quarter due to lost/stolen devices. Clients in the education sector also had a pronounced trend of cyberincidents stemming from employee accidental disclosures or lost devices, with approximately two-thirds of their incidents falling into these categories.

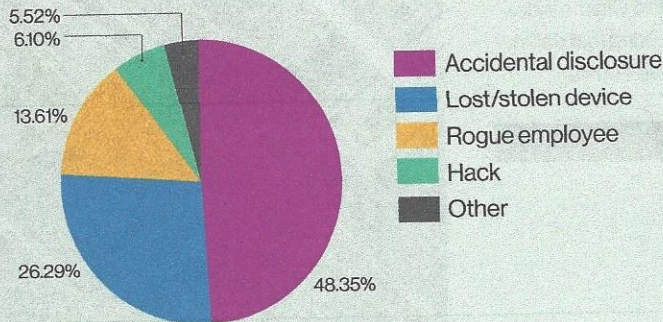


Claims included within the employee error or negligence category are those involving lost laptops or mobile devices, negligent disposal of paper records with PII in an unsecured manner, or personal files accidentally sent by email to an unintended recipient. Accordingly, it's important that organizations, especially those in the health care and education sectors, take special note of the risk caused by employee accidents and implement training and loss control measures focused on employee behavior.

Education industry
Percentage of claims by breach type



Healthcare industry
Percentage of claims by breach type



While accidental disclosures and lost devices together combine for the highest percentage of cyberincidents, the silver lining to this data is that the records lost in these claims represent less than 1% of the total records lost. To compare, hacks and third-party breaches account for approximately 90% of the total number of records lost. But that does not allay the concerns regarding employee conduct, as employees are most likely to be the source of the next cyberincident, and each incident can be costly.

Even though accidental disclosures and lost device cyberincidents generally do not result in high record loss cyber claims, the large quantity of claims may nevertheless prove costly — whether for a breach coach, legal costs, forensics or public relations — which may be less than the applicable self-insured retention (SIR) on a cyberinsurance policy. Depending on the insurer, the retention may apply to the number of individuals notified, the cost of the overall incident response, or both. This means an organization will have out-of-pocket costs for each of these events. That is not to mention the lost productivity cost associated with mitigating or remedying the breach.

For companies at a higher risk of multiple, low severity employee-based incidents, it may be advantageous to procure a cyberinsurance policy that provides consultative assistance from a breach coach (usually the most costly component of a low severity breach response) with no SIR.

In conclusion, the most common cyberincident that a company faces will be rooted in employee conduct, as borne out by the Willis Towers Watson Reported Claims Index. It is therefore crucial that organizations focus on cyber risk posed by its employees, and develop appropriate risk mitigation strategies, including encouraging regular security-conscious behavior and implementing continuing and regular awareness training.

Industry spotlight

Health care

By Gina Macari

The success of a business is increasingly defined by the strength of its technology, making data privacy and security a necessity and top priority for business survival. This is true for industries such as retail, education and hospitality, but no sector has felt the burden of the responsibility to protect private data more than the health care industry. Companies in the health care industry routinely maintain thousands of patient records containing the full spectrum of personally identifiable information and personal health information (PII and PHI) such as Social Security numbers, addresses, insurance policy numbers, medical diagnosis details and even credit card information. These organizations face vast exposure to privacy violation claims when systems are hacked, devices are stolen, or privacy procedures are thwarted — and even when employees make innocent mistakes.

The Willis Towers Watson Reported Claims Index reveals that the vast majority (81%) of claims made against health care organizations result from three breach types: (1) accidental disclosure of data (42%); (2) loss or theft of devices such as laptops and phones (26%); and (3) theft or misuse by rogue employees (13%). While hacks comprise only 6% of total breaches included in the Willis Towers Watson Reported Claims Index, hacks account for the highest number of records lost per breach. In fact, as shown in the chart on page 12, hacks represent the majority of the lost records containing PII and PHI. These observations are consistent with and supported by various other studies, such as IBM's 2016 Cyber Security Intelligence Index. In that study, which was based on data collected from between January 1, 2015 and December 13, 2015, IBM noted that more than 100 million health care records were compromised, and from more than 8,000 client devices in over 100 countries.²

With every lost record comes the possibility of exposure to a wide variety of claims and resulting costs. Aside from the potential reputational damage and loss of customer confidence, those organizations that have been victims of hackers have a profound understanding of the scope of financial liability that can result from being hacked. According to the "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data", a study commissioned by ID Experts, Ponemon Institute estimated that data breaches may cost the healthcare industry \$6.2 billion in 2016.³

One of those costs includes the fines and penalties levied by the U.S. Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA). In this regard, HHS's data reflects that HIPAA settlements are on the rise, largely due to the agency's aggressive enforcement proceedings against health care organizations. In the first 10 months of 2016 alone, the health care industry paid out just short of \$21 million to settle HIPAA violations.⁴

Top 10 HIPAA settlements (2014-2016)

Settlement (in millions)	Date
5.5	August 2016
4.8	May 2014
3.9	March 2016
3.5	November 2015
2.75	July 2016
2.7	July 2016
2.2	April 2016
2.14	October 2016
1.725	April 2014
1.55	March 2016

The \$5.5 million settlement in the above table involved an incident which began with the theft of laptops during a burglary at one of the company's facilities. Later, another laptop was stolen from an unlocked car. The investigation by HHS' investigative arm, the Office of Civil Rights (OCR), revealed that 2,000 patient records were potentially compromised, including the PHI of four million individuals. The \$5.5 million settlement reflects the government's goal to send a strong message to entities covered by HIPAA: that failure to comprehend the risk presented by stored PHI and take appropriate steps to protect it will not be excused.⁵

As a result of the increasing exposure to HIPAA fines and penalties, those in the business of managing risk in the health care space may find themselves searching for more answers to an old question:



How does cyberinsurance respond to HIPAA fines and penalties?

Many cyberinsurance policies expressly provide coverage for fines and penalties imposed by regulatory agencies, such as HHS, for violations of privacy laws.

A still lingering question, however, is whether HIPAA fines and penalties constitute uninsurable punitive damages. The answer to this question is unfortunately unclear and depends on a number of considerations, including whether: (1) the penalties are assessed for willful or intentional conduct; (2) the penalty is "punitive" rather than "compensatory;" and (3) the penalty is assessed directly against an Insured rather than vicariously.

To date, insurers have confirmed, through claim payments, that their intention is to cover HIPAA fines and penalties. While some cyberinsurance policies may include most favorable jurisdiction provision with respect to punitive damages, they are often silent regarding whether the same provision applies to HIPAA fines and penalties. As such, it is imperative that health care organizations work closely with their brokers to negotiate the most competitive wording available. Additionally, to the extent a court or insurance authority in a particular state could determine that portions of fines and penalties awards/assessments are uninsurable as a matter of public policy (based on any of the considerations above), organizations may also wish to consider obtaining fines and penalties wrap coverage offered through Bermuda markets. Because Bermuda markets are not subject to the same limitations regarding insurability of certain damages (e.g., choice of law under Bermuda policies tend to apply the Law of England and Wales, which is favorable to insurability of punitive damages) that are deemed punitive, the fines and penalties wrap policy coverage would "wrap-around" the primary domestic cyberinsurance policy and would fill any coverage gap in the event of a challenge on the grounds of insurability.

Finally, it is recommended that cyberinsurance policies contain coverage not only for the fines and penalties levied, but also for costs incurred in connection with the regulatory investigation of the alleged privacy violation, as these sums can be substantial.

² <http://www-03.ibm.com/security/data-breach/cyber-security-index.html>

³ <http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1>

⁴ <https://www.hhs.gov/ocr/newsroom/index.html>

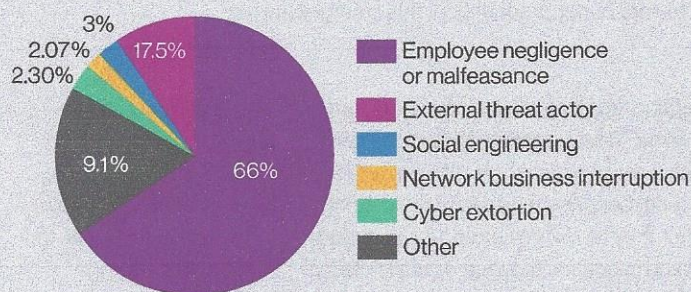
⁵ see footnote 4

The day the internet went missing

By Jim Devoe and Dan Twersky

A growing category of cyberincidents is Network Business Interruptions. While representing only 2.07% of incidents within the Willis Towers Watson Reported Claims Index, we see this category as increasingly significant. Not only do such claims have the possibility to result in catastrophic first- and third-party losses, but recent attacks have achieved far greater ingenuity and sophistication, creating new ways and tools for attackers to perpetrate such schemes.

Percentage of claims by breach type



The Dyn attack

A distributed denial of service (DDoS) attack against Dynamic Network Service, Inc. (Dyn), a major Domain Name Server host, created a wide ripple of disruption across the internet. DNS providers help ensure that an internet user ends up at the correct destination after entering a web address into their browser. The attack flooded Dyn's servers with so much traffic — reportedly 1 Terabit per second (akin to downloading the Library of Congress every two minutes) — that business customers who rely on Dyn to connect users to their sites, including major online social media, e-commerce, streaming video and audio, and content hosting companies, were disrupted to varying degrees. The sites were actually up and running, but merely appeared to be down.

Not only were the effects of this attack notable, so too was the source of the attack. Reportedly hundreds of thousands (if not tens of millions) of baby monitors, DVRs, security cameras and similar devices — collectively making up the internet of things (IoT) — were orchestrated to launch the simultaneous attack. Dyn advised the next day that the attack on their services came in three waves, none lasting more than two hours.

Business customers of Dyn reported similar disruptions as a consequence. A major cloud services provider advised that its service was affected during the first wave, for a similar timeframe. Others had differing impacts as the attack spread from the East Coast to West Coast and Europe. Customers of these businesses, in turn, felt the impact, whether it was the inconvenience of a streaming video being disrupted, or a business disruption arising from the inability to access the cloud provider's servers.

Finally, the manufacturer of the underlying technology common to many if not all of the devices leveraged in this attack, was forced to recall millions of their devices for upgrades.

How might cyberinsurance respond to an attack like this?

Network interruption

Known also as business interruption, this coverage provides an insured with coverage for lost earnings and extra expenses incurred due to an interruption of its own system. This coverage requires the insured to clear a waiting period — a minimum amount of time that must elapse before any interruption is covered. A typical waiting period is eight hours, but can vary depending on the type of business being insured.

Dependent network interruption

Similar to network interruption, this coverage provides insureds with protection when they suffer losses arising from a third-party system interruption. Using these events to illustrate, the insured here would be one of Dyn's customers, who themselves suffered a loss of earnings and/or incurred extra expense due to Dyn's systems being interrupted by the attack. The waiting period would be similar here, and other limitations may apply such as co-insurance or sublimits.

Breach response

For the insured which is directly attacked, breach response may provide some coverage for costs incurred. This coverage is usually thought of in the context of a privacy breach, and is generally tailored to related expenses such as the legal determination of privacy obligations state by state, notification of affected consumers, and the offering of credit/identity monitoring protection and fraud resolution services. While the attacks in this case were not privacy related, they nonetheless could trigger some additional aspects of breach response coverage including the costs of cyber forensics to "put out the fire," and the public relations costs intended to mitigate potential damage to the insured's brand and reputation.



Liability

Last but not least is liability coverage. Cyberinsurance policies will typically include liability coverage for claims alleging an insured's negligence in protecting systems and information. These claims can be from any affected party who can allege some level of damage, and can range from a single affected party (Dyn's direct customer, for instance) to a broad class action by downstream customers for the disruption of services for which they paid consideration. A second type of liability could arise if Dyn's commercial customers allege negligence in rendering agreed to professional services, violating contractually agreed upon and paid-for service levels.

Considerations and takeaways

Awareness

The emergence of the IoT leads to new variants of old threats. The notion that baby monitors could be unexpected participants in a massive DDoS attack such as this is alarming, and awareness that this is possible is important. As we understand how the IoT actually works — that these intelligent devices are basically miniature "PCs" with less control and visibility to their owners — it's not difficult to see how these devices could be hacked and misused. This recognition is a first step toward better preparing for this emerging threat.

Preparedness

Risk detection and mitigation steps by sophisticated tech companies limited the duration of loss suffered by these firms. The aforementioned cloud services provider, for instance, was able to re-direct to other service providers and minimize their reliance on Dyn during the attack, and the effective duration to them (and to their customers in turn). Clients should be asking themselves whether they are fully prepared for a similar threat; specifically whether the necessary risk detection and mitigation safeguards are in place.

Risk transfer

Cyberinsurance can provide a valuable and flexible tool for addressing many types of cyberlosses, and the attacks on Dyn are no exception. In fact, they underscore the need for Business Network Interruption coverage despite the historical low frequency of these types of attacks. Ensuring that Business Interruption coverage is in place in advance of a loss, that it includes the broadest possible terms and conditions, keeps up with rapid developments in these evolving areas of coverage, and is acted upon at the time of loss through proactive claims advocacy, are critical ingredients to successful risk transfer.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

As preliminary background, this case arises out of MBIC's refusal to pay an insurance claim made by Plaintiff, Bitpay, Inc. ("Bitpay"). See Doc. No. [1], p. 4, ¶¶19-22. Plaintiff alleges that its CFO received an email from someone asking for a comment on a bitcoin industry document. Id. p. 3, ¶12. In fact, the email was fraudulently sent from a hacked account. Id. p. 3, ¶13. After Bitpay's CFO entered his credentials on a website controlled by the hacker, the hacker

was able to send false authorizations to Bitpay, causing the transfer and loss of \$1,850,000 in bitcoin. Id. pp. 3-4, ¶¶14-17. Because Defendant refused to insure the loss, Plaintiff filed the present complaint, asserting two counts: (1) that the refusal to pay the claim was a breach of Plaintiff's insurance policy and (2) that the refusal to pay was done in bad faith. Id. pp. 5-6, ¶¶27-36.

In conjunction with its answer, Defendant filed the present motion, requesting that the Court try bifurcate the two counts, and that the Court stay discovery on the bad-faith claim pending resolution of the breach-of-contract claim. See Doc. No. [8]. Federal Rule of Civil Procedure 42(b) provides the Court with the authority to bifurcate the trial of separate claims in the interest of "convenience, to avoid prejudice, or to expedite and economize." Fed. R. Civ. P. 42(b). "The decision to bifurcate is committed to the sound discretion of the trial court." Home Elevators, Inc. v. Millar Elevator Serv. Co., 933 F. Supp. 1090, 1091 (N.D. Ga. 1996). Bifurcation is "not the usual course that should be followed." Id. The burden to show that bifurcation is warranted is on the party requesting bifurcation. Id.

Here, Defendant notes that, under Georgia law, Plaintiff must first prove that its loss was covered by the insurance policy before it can prove that MBIC's

refusal to pay Plaintiff's claim was in bad faith. See Doc. No. [8], p. 3; see also O.C.G.A. § 33-4-6 (providing for attorney's fees and increased damages where an insurer makes a bad faith refusal to pay "a loss which is covered by a policy of insurance"). Thus, Defendant argues, needless expense may be prevented by staying discovery on the bad-faith count until there has been a determination as to whether Plaintiff's loss was even covered by the insurance policy. See Doc. No. [8], p. 4. Plaintiff responds, in part, that the facts underlying both the bad-faith claim and the breach-of-contract claim "are inextricably intertwined" and that staying discovery on the bad-faith claim would result in a "duplication of efforts," which would "increase the cost of discovery exponentially" and require the Court to "resolve discovery disputes piecemeal." Doc. No. [9], pp. 9-10. The Court agrees with Plaintiff that denying the motion to stay and proceeding with discovery on the bad-faith claim is the most efficient way to proceed in this case.

The bulk of Plaintiff's requests for production are for documents directly related to Plaintiff's claim, such as "communications regarding the commercial crime coverage," evidence relating to "the underwriting and/or actuarial analysis of the Policy," and MBIC's claim file or other documents relating to

MBIC's investigation of the claim. See Doc. No. [18-3], pp. 6-7. In a letter concerning the present discovery dispute, defense counsel asserted that such evidence is "inappropriately directed to claims handling/bad faith and not the coverage determination made by the claims department." See Exhibit A,¹ p. 1. While the requests are surely relevant to the bad-faith claim, some of the requests are also relevant to the breach-of-contract claim. In particular, MBIC's claim file seems directly relevant to "the coverage determination made by the claims department."

If the Court were to grant the Motion to Bifurcate and Stay Discovery, the Court would be required to parse each and every request for production, not to mention each question Plaintiff might potentially ask during a deposition, to determine if it "related to" the breach-of-contract claim or the bad-faith claim — or, if the request related to both claims, how to properly limit the request to only reach information related to the breach-of-contract claim. Such an exercise in hair-splitting would waste precious judicial resources, and result in unnecessarily duplicative discovery if Plaintiff in fact succeeds in proving that

¹ Defendant's letter to Plaintiff concerning the present discovery dispute was provided to the Court in advance of the conference call on this dispute. It is attached to this Order as Exhibit A, and is referred to as such throughout the Order.

the loss was covered. The increased discovery burden on Defendant is minimal since many, if not most, of the requests and potential deposition questions will relate to both claims. The facts demonstrating whether the loss is covered by the policy and the facts underlying MBIC's decision not to pay the claim will clearly overlap substantially. Simply put, Defendant has not met its burden of showing that bifurcation is warranted in this case. See Home Elevators, Inc., 933 F. Supp. at 1091.

Having decided that the most efficient course of conduct in this case is to allow discovery on both of Plaintiff's claims, the Court now turns to the particular discovery dispute at hand. During the conference call, Defendant's arguments centered largely around its contention that the information requested by Plaintiff is "irrelevant." However, Plaintiff's requests for "communications regarding the commercial crime coverage"—the provision at issue in this case—as well as for evidence relating to "the underwriting and/or actuarial analysis of the Policy," and MBIC's claim file or other documents relating to MBIC's investigation of the claim, are quite clearly relevant to the issues in this case. See Doc. No. [18-3], pp. 6-7. Defendant may, and in fact did, dispute whether such requests are "directed to" the bad-faith claim or the

breach-of-contract claim, but the requests are relevant. See Exhibit A, p. 1. Defendant's communications regarding the policy provision at issue, its underwriting analysis, its claim file, and most of the other production requests will tend to either prove or disprove Plaintiff's claim that Defendant refused to pay a claim that it knew was covered by the policy.

Although not discussed during the conference call, Defendant, in its letter to Plaintiff regarding the discovery dispute, also objected to Plaintiff's request for documents related to "Social Engineering Endorsements," because that product was not offered at the time of Bitpay's contract with MBIC, and thus is not at issue in this case. Id. p. 2. The Court agrees. Information regarding Defendant's other products, developed after the contract at issue in this case, is not relevant to the issue of whether Defendant breached its contract with Plaintiff. Nor is it relevant to the issue of whether Defendant's decision to deny Bitpay's claim was in bad faith. Thus, Plaintiff's Request for Production number 18 is beyond the scope of permissible discovery in this case. See Doc. No. [18-3], p. 8.

Defendant also objects to Plaintiff's requests for documents related to claims by other individuals handled by Defendant. Such evidence is relevant to the extent that it could show whether Defendant chose to pay or deny other

claims that are factually similar to Plaintiff's claim. Defendant's stronger objection is that production of such evidence may be overly burdensome. Even potentially relevant evidence may be beyond the scope of discovery. Discovery must be "proportional to the needs of the case," and the Court must consider "whether the burden or expense of the proposed discovery outweighs its likely benefit." Fed. R. Civ. P. 26(b)(1). This issue concerns two of Plaintiff's Requests for Production: numbers 20 and 21. See Doc. No. [18-3], pp. 8-9.

Request for Production number 20 asks for all documents "relating to coverage under MBIC's commercial crime policies for fraudulent transfers occurring after receipt by the insured a fraudulent instructions from a third party." Id. p. 8. This request is carefully tailored to the particular facts of this case, and thus is highly relevant to the issues in the case at bar. See Doc. No. [1], pp. 3-4, ¶¶12-17. Thus, the burden or expense of producing the evidence is not outweighed by its likely benefit. See Fed. R. Civ. P. 26(b)(1). Defendant would only have to produce evidence of claims similar to Bitpay's claim, and, because the claims would be similar, they would be highly relevant.

Plaintiff's Request for Production number 21, in contrast, is overly broad. In request 21, Plaintiff asks for all documents "relating to coverage under MBC's

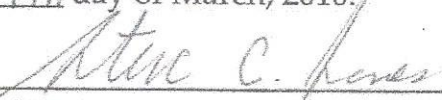
commercial crime policies for losses or claims resulting from (in whole or in part) the hacking of a computer system hosting services for an insured.” Doc. No. [18-3], p.9. This would require Defendant to produce evidence of any and every claim in which a computer system hosting services for an insured was hacked, without regard to the manner or method in which the system was hacked. Probative value of the evidence to be produced would almost certainly be outweighed by the undue burden of producing such voluminous discovery. Accordingly, Request for Production number 21 is beyond the permissible scope of discovery, as currently phrased. The Court will allow Plaintiff to rephrase the request, if it so chooses, to make the request more narrowly tailored to the particular facts of this case.

For the reasons given above, Defendant’s Motion to Bifurcate and to Stay Discovery on the bad-faith claim (Doc. No. [8]) is **DENIED**.² With the exceptions of Plaintiff’s Requests for Production numbers 18 and 21, as explained above, Defendant is hereby **ORDERED** to produce all discovery responsive to Plaintiff’s

² While the Court is denying the Motion to Bifurcate at the discovery stage, the Court is not ruling on whether to bifurcate the claims at trial. Allowing discovery on both claims allows for the most expedient resolution of this case, but trying the bad-faith claim and the breach-of-contract claim together may result in undue prejudice, and thus warrant bifurcation. See Fed. R. Civ. P. 42(b).

other requests. If Defendant intends to withhold any information on the grounds that it is privileged, it must do so in compliance with Fed. R. Civ. P. 26(b)(5). Each side will bear its own costs and attorneys' fees incurred as a result of this discovery dispute.

IT IS SO ORDERED, this 17th day of March, 2016.



HONORABLE STEVE C. JONES
UNITED STATES DISTRICT JUDGE

Josh Nazarian, one of the managing directors for Principle [Doc. No. 22-7, ¶ 2, admitted; Doc. No. 22-3, p. 6]. The email appeared to have been sent from his corporate email address [Id.]. The email referenced a company acquisition and instructed the controller to “treat the matter with the utmost discretion” [Doc. No. 22-7, ¶ 3, admitted; Doc. No. 22-3, p. 6]. The email also instructed the controller to work with an attorney, Mark Leach, to “ensure that the wire goes out today” [Id.]. Mr. Nazarian was not in the office on the day of the fraudulent email [Doc. No. 22-7, ¶ 4, admitted]. He did not send the email [Doc. No. 22-7, ¶ 5, admitted].

Later that morning, the controller received an email from a “Mark Leach” who represented himself to be a partner at Alston & Bird [Doc. No. 22-7, ¶ 6, admitted; Doc. No. 22-3, p. 9]. Mr. Leach stated that he was reaching out at the request of Mr. Nazarian [Id.]. Mr. Leach also sent wiring instructions to a bank in China [Id., Doc. No. 22-3, p. 11]. At 10:15am, Mr. Leach called the controller and emphasized that they needed to complete the wire transaction that day and that he had Mr. Nazarian’s full approval to execute the wire [Doc. No. 22-7, ¶ 8, admitted].

The controller was not able to forward an email to the financial institution to wire the funds because the institution required more than an email to wire funds

from an account [Doc. No. 22-7, ¶ 9, admitted]. So, the controller logged into the company's online account to enable the approval function and to verify the capability to wire internationally in different forms of currency [Doc. No. 22-7, ¶ 10, admitted]. She then called Mr. Leach to confirm the capability and instructed another Principle employee to create the wire instructions [Doc. No. 22-7, ¶ 11, admitted]. The controller then approved the wire [Doc. No. 22-7, ¶ 12, admitted].

The financial institution's fraud prevention unit called and emailed the controller requesting verification of the wire [Doc. No. 22-7, ¶ 13, admitted]. The financial institution requested the controller to verify how Mr. Leach had received the wire instructions [Doc. No. 22-7, ¶ 14, admitted]. The controller called Mr. Leach and was told he verbally received the wire instructions from Mr. Nazarian [Doc. No. 22-7, ¶ 15, admitted]. The controller relayed this information to the financial institution, and the financial institution released the wire [Doc. No. 22-7, ¶ 16, admitted].

The next day, the controller spoke with Mr. Nazarian and told him that the wire had been made in accordance with his instruction [Doc. No. 22-7, ¶ 17, admitted]. Mr. Nazarian had no knowledge of the emails, Mr. Leach, or the wire

instructions, and he immediately called the fraud department of the financial institution to report the fraud [Doc. No. 22-7, ¶ 18, admitted]. Neither the financial institution nor law enforcement were able to recover the funds [Doc. No. 22-7, ¶ 19, admitted]. Principle suffered a \$1.717 million loss [Doc. No. 22-7, ¶ 20, admitted].

Principle is the named insured under Commercial Crime Policy No. 001512502 for the policy period of December 20, 2014 to December 20, 2015 [Doc. No. 22-7, ¶ 21, admitted]. Principle paid the premium for the Commercial Crime Policy [Doc. No. 22-7, ¶ 22, admitted]. The Commercial Crime Policy provides coverage for specifically-defined categories of crimes, one of which is “Computer and Funds Transfer Fraud” [Doc. No. 22-7, ¶ 23, admitted]. The “Limit of Insurance” is \$5,000,000 per occurrence with a \$25,000 deductible per occurrence [Id.].

Specifically, Section A.6 of the Commercial Crime Policy states:

- a. We will pay for:
 - (2) Loss resulting directly from a “fraudulent instruction” directing a “financial institution” to debit your “transfer account” and transfer, pay or deliver “money or “securities” from that account.

[Doc. No. 22-4, p. 7]. The Commercial Crime Policy further provides various definitions in Section F, including the following:

9. "Financial institution" means:
 - b. With regard to Insuring Agreement A.6:
 - (1) A bank, savings bank, savings and loan association, trust company, credit union or similar depository institution;
 - (2) An insurance company; or
 - (3) A stock brokerage firm or investment company.
12. "Fraudulent instruction" means:
 - a. With regard to Insuring Agreement A.6.a.(2):
 - (1) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic instruction directing a "financial institution" to debit your "transfer account" and to transfer, pay or deliver "money" or "securities" from that "transfer account", which instruction purports to have been issued by you, but which in fact was fraudulently issued by someone else without your knowledge or consent.
 - (2) A written instruction (other than those covered by Insuring Agreement A.2.) issued to a "financial institution" directing the "financial institution" to debit your "transfer account" and to transfer, pay or deliver "money" or "securities" from that "transfer account", through an electronic funds transfer system at specified times or under specified conditions, which instruction purports to have been issued by you, but which in fact was issued, forged or altered by someone else without your knowledge or consent.
 - (3) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic or written instruction initially received by you, which instruction purports to have been issued by an "employee", but which in fact was fraudulently issued by someone else without your or the "employee's" knowledge or consent.
16. "Money" means:

- a. Currency, coins and bank notes in current use and having a face value;
- b. Traveler's checks and money orders held for sale to the public; and
- c. In addition, includes:
 - (1) Under Insuring Agreements A.1. and A.2., deposits in your account at any financial institution; and
 - (2) Under Insuring Agreement A.6., deposits in your account at a "financial institution" as defined in Paragraph F.9.b.

[Doc. No. 22-4, pp. 16-19].

Principle notified Ironshore of its claim consistent with the terms of the Policy [Doc. No. 22-7, ¶ 26, admitted]. Thereafter, Principle submitted a Sworn Proof of Loss to Ironshore under the Commercial Crime Policy, which it later amended, seeking coverage under the Commercial Crime Policy [Doc. No. 22-7, ¶ 27, admitted]. Ironshore denied coverage for the claim on July 24, 2015 [Doc. No. 22-7, ¶ 29, admitted].

On October 20, 2015, Principle filed this action in the Superior Court of Fulton County, Georgia [Doc. No. 1-2]. The action was removed to this Court on November 25, 2015, based on this Court's diversity jurisdiction. The Complaint alleges claims for Breach of Contract and Bad Faith pursuant to O.C.G.A. § 33-4-6 [Doc. No. 1-2].

II. Plaintiff's Motion to Exclude [Doc. No. 38]

Plaintiff Principle has moved the Court to exclude Exhibit 2 [Doc. Nos. 30-2 and 32-4], which was submitted by Ironshore in support of its summary judgment briefing. Principle contends that Ironshore has failed to properly authenticate the document. Principle also contends that Exhibit 2 should be excluded because it is not relevant, and even if it was, it should be excluded pursuant to Federal Rule of Evidence 403. Finally, Principle contends that the document was not properly provided according to Local Rule 56.1.

Exhibit 2 is a document that purports to be an endorsement and is titled "Add Cyber Deception Coverage." Ironshore argues that this exhibit is provided as an illustration of the type of policy language which may provide coverage for this type of claim and that it is merely an aid for the Court in construing the Policy language. The Court agrees with Principle that Exhibit 2 is not relevant. The endorsement is not part of the Policy at issue in this case. Also, it appears to be dated March 2015, and there is no evidence that Ironshore has sought or received approval from the Georgia Department of Insurance to use the endorsement in Georgia. It is not relevant to determining coverage under this Policy and is not

relevant to the coverage issued raised by the parties. As such, Plaintiff's Motion to Exclude [Doc. No. 38] is GRANTED.

III. Plaintiff's Motion for Judicial Notice [Doc. No. 39]

Plaintiff Principle has moved the Court to take judicial notice of certain filings made with the Georgia Department of Insurance [Doc. No. 39]. Specifically, Principle requests that the Court take judicial notice of the following facts: (1) Form SURE-130089150 was drafted by The Surety & Fidelity Association of America and was filed with the Georgia Department of Insurance because it was located in the Department's SERFF database; and (2) Ironshore's Exhibit 2 [Doc. Nos. 30-2 and 32-4] was not filed with the Georgia Department of Insurance because it cannot be located in their SERFF database.

As to the first fact, Ironshore does not oppose Plaintiff's Motion, and Plaintiff's Motion [Doc. No. 39] is GRANTED as to that fact. The Court will take judicial notice that Form SURE-130089150 was drafted by The Surety & Fidelity Association of America and was filed with the Georgia Department of Insurance. The Court also takes judicial notice of its contents.

As to the second fact, Ironshore contends that this fact is not relevant to any issue in this case. As discussed above, the Court agrees. The cyber-deception

endorsement is not a part of the Commercial Crime Policy issued by Ironshore to Principle. Accordingly, whether or not the endorsement has been filed or approved for use in Georgia is irrelevant to the issue of whether the Policy covered the loss in this case. As to the second fact, Plaintiff's Motion [Doc. No. 39] is DENIED.

For the reasons stated above, Plaintiff's Motion for Judicial Notice [Doc. No. 39] is GRANTED in part and DENIED in part. The Court will take judicial notice of the first fact but not the second.

IV. Motions for Summary Judgment [Doc. Nos. 22 and 32]

The parties have filed cross-motions for summary judgment regarding the scope of the insurance coverage at issue. The material facts of the case outlined above are agreed upon by the parties, so there are no issues of material fact. Thus, a legal determination is needed as to whether the fraud in question is covered by the Policy.

A. Legal Standard

Federal Rule of Civil Procedure 56 requires that summary judgment be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. P.

56(a). “The moving party bears ‘the initial responsibility of informing the . . . court of the basis for its motion, and identifying those portions of the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, which it believes demonstrate the absence of a genuine issue of material fact.’” Hickson Corp. v. N. Crossarm Co., 357 F.3d 1256, 1259 (11th Cir. 2004) (quoting Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986) (internal quotations omitted)). Where the moving party makes such a showing, the burden shifts to the non-movant, who must go beyond the pleadings and present affirmative evidence to show that a genuine issue of material fact does exist. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 257 (1986). The applicable substantive law identifies which facts are material. Id. at 248. A fact is not material if a dispute over that fact will not affect the outcome of the suit under the governing law. Id. An issue is genuine when the evidence is such that a reasonable jury could return a verdict for the non-moving party. Id. at 249-50.

In resolving a motion for summary judgment, the court must view all evidence and draw all reasonable inferences in the light most favorable to the non-moving party. Patton v. Triad Guar. Ins. Corp., 277 F.3d 1294, 1296 (11th Cir. 2002). But, the court is bound only to draw those inferences that are

reasonable. “Where the record taken as a whole could not lead a rational trier of fact to find for the non-moving party, there is no genuine issue for trial.” Allen v. Tyson Foods, Inc., 121 F.3d 642, 646 (11th Cir. 1997) (quoting Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986)). “If the evidence is merely colorable, or is not significantly probative, summary judgment may be granted.” Anderson, 477 U.S. at 249-50 (internal citations omitted); see also Matsushita, 475 U.S. at 586 (once the moving party has met its burden under Rule 56(a), the nonmoving party “must do more than simply show there is some metaphysical doubt as to the material facts”).

B. Analysis - Coverage

Principle contends that the loss at issue is covered by Section A.6.a.(2). of the Commercial Crime Policy which provides coverage for loss “resulting directly from a ‘fraudulent instruction’ directing a ‘financial institution’ to debit your ‘transfer account’ and transfer, pay or deliver ‘money’ or ‘securities’ from that account.” Principle argues that its loss resulted directly from the fraudulent email that appeared to have been sent by Mr. Nazarian. In support of its denial of coverage, Ironshore argues that the loss did not result “directly” because: (1) additional information for the wire was conveyed to Principle by Mr. Leach after

the initial email, and (2) Principle's employees set up and approved the wire transfer.

The Court finds that the language of the provision at issue is ambiguous. "When the language of an insurance contract is ambiguous and subject to more than one reasonable construction, the policy must be construed in the light most favorable to the insured, which provides him with coverage." Western Pacific Mut. Ins. Co. v. Davies, 601 S.E.2d 363, 369 (Ga. Ct. App. 2004). It is reasonable for Plaintiff to interpret the language of the policy to provide coverage even if there were intervening events between the fraud and the loss. Defendant's interpretation, which would require an immediate link between the injury and its cause, is also reasonable. In this circumstance, the Court must construe the policy in the light most favorable to Plaintiff and provide coverage. This is consistent with the District Court's decision in Apache Corp. v. Great Am. Ins. Co., Civil Action No. 4:14-CV-237, 2015 WL 7709584, at *3 (S.D. Texas Aug. 7, 2015), in which the Court stated that adopting the insurance company's reading would be "to limit the scope of the policy to the point of almost non-existence." As in Apache, Plaintiff here could act only through its officers and employees. If some employee interaction between the fraud and the loss was sufficient to allow

Defendant to be relieved from paying under the provision at issue, the provision would be rendered “almost pointless” and would result in illusory coverage. Id.

As to coverage, Plaintiff’s Motion for Partial Summary Judgment [Doc. No. 22] is GRANTED, and Defendant’s Motion for Summary Judgment [Doc. No. 32] is DENIED as moot.

C. Analysis - Bad Faith

Defendant has also moved for summary judgment as to Plaintiff’s bad faith claim. O.C.G.A. § 33-4-6 provides the exclusive remedy for an insured’s bad faith refusal to pay insurance proceeds. Great Southwest Express Co. v. Great Am. Ins. Co., 665 S.E.2d 878 (Ga. Ct. App. 2008). For Plaintiff to prevail on a claim for bad faith, it must prove: (1) that the claim is covered under the Policy; (2) that a demand for payment was made against the insurer within 60 days prior to filing suit; and (3) that the insurer’s failure to pay was motivated by bad faith. Lawyers Title Ins. Co. v. Griffin, 691 S.E.2d 633, 636 (Ga. Ct. App. 2010) (citation omitted).

To determine whether the insurer engaged in bad faith, an insured must show by evidence that “under *the terms of the policy* upon which the demand is made and under the facts surrounding the response to that demand, the insurer had

no 'good cause' for resisting and delaying payment." Id. (citing Georgia Intl. Life Ins. Co. v. Harden, 280 S.E.2d 863, 866 (Ga. Ct. App. 1981) (emphasis in original)). Courts grant summary judgment to insurers on bad faith claims where the issue of liability was close. See, e.g., Homick v. Am. Casualty Co., 433 S.E.2d 318, 319 (affirming grant of summary judgment to insurer on bad faith: "Ordinarily, the question of good or bad faith is for the jury, but when there is no evidence of unfounded reason for the nonpayment, or if the issue of liability is close, the court should disallow imposition of bad faith penalties. Good faith is determined by the reasonableness of nonpayment of a claim.") (quoting Intl. Indem. Co. v. Collins, 367 S.E.2d 786, 786 (Ga. 1988))).

The Court finds that the issue of liability was close in this case. It was not "unreasonable" or "unfounded" for Defendant to deny coverage here and wait for this Court to determine the coverage required by the contract. As such, Defendant is entitled to summary judgment on Plaintiff's bad faith claim, and its Motion for Summary Judgment [Doc. No. 32] as to the bad faith claim is GRANTED.

VI. Conclusion

For the reasons stated above, Plaintiff's Motion to Exclude [Doc. No. 38] is GRANTED. Plaintiff's Motion for Judicial Notice [Doc. No. 39] is GRANTED

in part and DENIED in part. As to coverage, Plaintiff's Motion for Partial Summary Judgment [Doc. No. 22] is GRANTED, and Defendant's Motion for Summary Judgment [Doc. No. 32] is DENIED as moot. As to the bad faith claim, Defendant's Motion for Summary Judgment [Doc. No. 32] is GRANTED. The Clerk is DIRECTED to enter judgment and close this action.

SO ORDERED, this 30th day of August, 2016.



RICHARD W. STORY
United States District Judge

