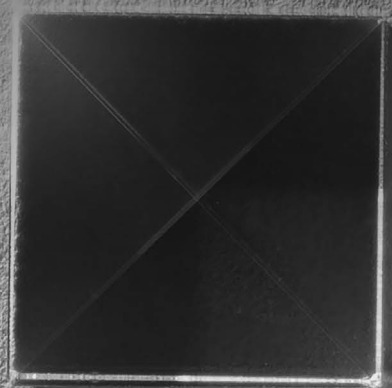
THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

ALTERNATIVE RISKS

Seeing around the cyber-corner: What's next for cyberliability policies?

KARIN S. ALDAMA | TRED R. EYERLY
RINA CARMEL



ALTERNATIVE CAPITAL MARKETS

#49 APRIL 2019

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

ALTERNATIVE MODELS

ALTERNATIVE RISKS

ALTERNATIVE MARKETS

DEAR READER,

Welcome to edition 49 of the Capco Institute Journal of Financial Transformation.

Disruptive business models are re-writing the rules of our industry, placing continuous pressure on financial institutions to innovate. Fresh thinking is needed to break away from business as usual, to embrace the more rewarding, although more complex alternatives.

This edition of the Journal looks at new digital models across our industry. Industry leaders are reaching beyond digital enablement to focus on new emerging technologies to better serve their clients. Capital markets, for example, are witnessing the introduction of alternative reference rates and sources of funding for companies, including digital exchanges that deal with crypto-assets.

This edition also examines how these alternatives are creating new risks for firms, investors, and regulators, who are looking to improve investor protection, without changing functioning market structures.

I am confident that you will find the latest edition of the Capco Journal to be stimulating and an invaluable source of information and strategic insight. Our contributors are distinguished, world-class thinkers. Every Journal article has been prepared by acknowledged experts in their fields, and focuses on the practical application of these new models in the financial services industry.

As ever, we hope you enjoy the quality of the expertise and opinion on offer, and that it will help you leverage your innovation agenda to differentiate and accelerate growth.

Lance Levy, **Capco CEO**

SEEING AROUND THE CYBER-CORNER: WHAT'S NEXT FOR CYBERLIABILITY POLICIES?[1]

KARIN S. ALDAMA | Partner, Perkins Coie LLP
TRED R. EYERLY | Director, Damon Key Leong Kupchak Hastert
RINA CARMEL | Senior Counsel, Anderson, McPharlin & Conners LLP

ABSTRACT

Cybersecurity coverage issues began to arise 20-25 years ago, when computers started becoming ubiquitous in the workplace. Initially, insureds sought coverage for cyber incidents under traditional policies, which led to somewhat metaphysical coverage issues like: what is data, exactly? Is it tangible property for purposes of CGL policies? Is data loss a direct physical loss covered under first-party property policies? The first cyber policy written to provide clarity on these issues and provide coverage specifically for cyber risks was introduced in 1997. But cyber policies, which are not standardized, raise different issues, such as the scope of coverage, which may develop more slowly than the risks of the cyberworld; whether the failure by an insured to implement cybersecurity measures may be grounds to disclaim coverage; and how novel policy language is to be construed. This article traces the historical coverage analyses, to set the stage for a discussion of common provisions of cyberliability coverages available today and the related issues that have arisen or may arise. It also discusses the slowly developing case law addressing cyber policies, and assesses what coverage and bad faith arguments and defenses may be raised as such policies continue to be addressed in the courts.

1. INTRODUCTION

Cybersecurity coverage issues began to arise approximately twenty to twenty-five years ago, when computers started becoming ubiquitous in the workplace. Historically, the coverage issue was metaphysical in nature: what is data, exactly? Could data constitute tangible property, for coverage under traditional CGL policies? Could data loss constitute a direct physical loss, for coverage under first-party property policies? These issues continue to arise today, as not all insureds purchase cyberliability policies, and instead – or in addition – may seek coverage under traditional policies in case of a cyber breach.[2]

Modern cyberliability policies are usually written to avoid this quandary. Different issues arise, though. These issues include the scope of coverage, which may develop more slowly than the risks of the cyberworld; whether any failure by the insured to implement cybersecurity measures may be grounds to disclaim coverage; and the impact of the novelty of policy terms and risks.

[1] Originally published in the Spring 2018 edition of Insurance Coverage, copyright 2018 American Bar Association. This article is partly based on Aldama, K. S., and T. R. Eyerly, 2018, "Cyber policies – the next wave," ABA Insurance Coverage Litigation Committee CLE Seminar, March. This article does not provide legal advice, and a given situation may vary from the facts discussed in this article. The views and opinions expressed in this article do not necessarily reflect the opinions of all of its authors on everything expressed herein, nor of their firms or clients.

[2] E.g., Zurich Am. Ins. v. Sony Corp. of Am., Index No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Cty. Feb. 21, 2014) (ruling no duty to defend underlying action alleging hacking of PlayStation online services existed under CGL policy).

This article traces the historical coverage analyses, as an aid to today's insurers, insureds, and coverage counsel. Next, it reviews common provisions of cyberliability coverages available today and the related issues that have arisen. Finally, now that some cyberliability coverage suits have been filed, the authors gaze into their crystal ball to see what coverage and bad faith arguments and defenses may be raised.

2. HISTORICAL AND CURRENT COVERAGE CASE LAW UNDER TRADITIONAL POLICIES

2.1 Traditional CGL policies

Traditional CGL policies usually provide coverage under Coverage A for "property damage," defining that term to require damage to tangible property.[3] ISO main forms dated 2004 and later provide that "electronic data is not tangible property."[4] As of May 1, 2014, ISO introduced optional forms, for use with CGL and general excess policies excluding coverage for risks of data breaches, disclosure of a third party's personal or confidential information, and notification and credit monitoring for individuals whose information was compromised.[5] These forms apply to both Coverage A and Coverage B.[6] A software exclusion, barring coverage for "personal and advertising injury" "[a]rising out of: (d) Computer code, software or programming used to enable: (i) Your web site; or (ii) The presentation or functionality of an 'advertisement' or other content on your web site," was recently held unambiguous, although the underlying action involved unauthorized distribution of software rather than a data breach.[7]

Even before these relatively recent policy terms and endorsements were introduced, many courts were reluctant to find that losses due to cyber breaches were covered under Coverage A.

One of the earliest cyber coverage cases, Seagate Technology, Inc. v. St. Paul Fire and Marine Ins. Co.,[8] involved underlying allegations that the third-party claimant had incorporated the insured's defective drives into its computers. Because the drives were not inherently dangerous products, and the underlying complaint did not allege resulting damage to other parts of the third-party claimant's computers, the CGL policy's "property damage" provisions were not satisfied, and the insurer had no duty to defend. Underlying allegations of loss of the third-party claimant's customers' information, and loss of business and damage to the third-party claimant's reputation, were not sufficient to create a duty to defend.[9] The court's reasoning was implicitly based on a requirement of damage to tangible property, as the court cited to principles from cases involving asbestos and construction defect coverage.[10]

In contrast to Seagate, America Online, Inc. v. St. Paul Mercury Insurance Co.[11] involved underlying allegations that incorporation of the insured's defective software caused resulting damage to the third-party claimants' computers. Specifically, the insured's software allegedly contained bugs that were incompatible with the third-party claimants' other software and operating systems, altering their software, disrupting network connections, causing the loss of stored data, and causing their operating systems to crash. Under the ordinary meaning of "tangible," "the physical magnetic material on the hard drive that retains data, information, and instructions is tangible property."[12] However, the court stated that this did not equate to a conclusion that "data, information, and instructions, which are codified in a binary language for storage on the hard drive, are tangible property."[13] The court concluded that they are not, and moreover, alteration of data, information, and instructions does not cause damage to the hard, tangible parts of a computer.[14] Thus, the insurer had no duty to defend.[15]

Coverage B, in contrast, does not require tangible property, but instead may provide coverage for specifically enumerated offenses.[16] Thus, data breaches have been found potentially covered under some CGL policies, especially those with non-standard language. In Hartford

[3] E.g., ISO Form No. CG 00 01 04 13 at 15.
[4] ISO Form Nos. CG 00 01 12 04 at 15, CG 00 01 12 07 at 15, CG 00 01 04 13 at 15.
[5] ISO, 2013, "Access or disclosure of confidential or personal information exclusions introduced," Commercial lines forms filing CL-2013-ODBFR at 3; ISO, 2013, "Access or disclosure of confidential or personal information exclusions introduced," Commercial general liability forms filing GL-2013-ODBFR; Ron Biederman, R., 2014, "ISO comments on CGL endorsements for data breach liability exclusions," Insurance Journal, July 18, https://bit.ly/2TVay4h (commenting on forms CG 21 06 05 14, CG 21 07 05 14, and CG 21 08 05 14).
[6] See n.5, supra.
[7] BF Advance, LLC v. Sentinel Ins. Co., No. 16-CV-5931-KAM-JO, 2018 WL 4210209, at *10-12 (E.D.N.Y. Mar. 20, 2018).
[8] 11 F. Supp. 2d 1150 (N.D. Cal. 1998).
[9] Id. at 1155.
[10] Id. at 1154-56 (citing cases including Armstrong World Indus., Inc. v. Aetna Cas. & Sur. Co., 45 Cal. App. 4th 1 (1996) and New Hampshire Ins. Co. v. Vieira, 930 F.2d 696 (9th Cir. 1991)).
[11] 347 F.3d 89 (4th Cir. 2003) (Virginia law).
[12] Id. at 94-95 (citing Webster's Third New International Dictionary of the English Language Unabridged 2337 (1993) for definition of "tangible" as "capable of being touched: able to be perceived as materially existent esp. by the sense of touch: palpable, tactile" and for definition of "tangible property" as "having physical substance apparent to the senses.").
[13] Id. at 95.
[14] Id. at 94-97.
[15] The court also held that the impaired property exclusion barred coverage. Id. at 97-99.
[16] E.g., ISO Form No. 00 01 04 13 at 6, 15.

Casualty Insurance Co. v. Corcino & Associates,[17] the third-party claimants alleged that the insured's job applicant posted their private, confidential, and sensitive medical and psychiatric information, which the co-defendant hospital had provided to the insured. The CGL policy at issue provided coverage for "electronic publication of material that violates a person's right of privacy."[18] The insurer did not dispute that the allegations fell within this coverage provision. The insurer argued, instead, that the policy's exclusion for "personal and advertising injury" "[a]rising out of the violation of a person's right to privacy created by any state or federal act" barred coverage. The court disagreed, concluding that the insured's argument, namely, that the rights to privacy were not created by state or federal acts, but rather by constitutional and common law principles, was reasonable.[19] The court rejected the insurer's argument that the insureds were in fact suing under state statutes, reasoning that those statutes codified constitutional and common law principles.[20]

In Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC,[21] the underlying class members alleged that the insured, which was in the business of safekeeping medical records for its healthcare provider customers, posted their confidential medical records on the internet, such that they became publicly accessible. The non-standard CGL policies provided coverage for "electronic publication of material that … gives unreasonable publicity to a person's private life" (for the 2012 policy) and "electronic publication of material that ... discloses information about a person's private life (for the 2013 Policy)."[22] The policies did not define the term "publication." The court concluded that "exposing confidential medical records to online searching is 'publication,'" and because medical records were at issue, the publicity was "unreasonable."[23] Thus, the insurer had a duty to defend.

On the other hand, hackers' appropriation of third-party claimants' personal private information (PPI) from the insured's web portal was held not to constitute a "publication" in Innovak International, Inc. v. Hanover Insurance Co.[24] The policy at issue defined "personal and advertising injury" to mean "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[25] The court held that there was no potential for coverage, explaining that the insureds did not disseminate the third-party claimants' PPI, and the insureds' publication of software did not violate the third-party claimants' privacy.[26]

2.2 Traditional property policies

Traditional property policies usually require "direct physical loss."[27] Courts have come to divergent conclusions as to whether data is physical, although courts seem to be more likely to find that data is "physical" under a property policy than to find it is "tangible" property under a CGL policy.

In Ward General Insurance Services, Inc. v. Employers Fire Insurance Co.,[28] the court ruled that a database crash was not covered because there was no "direct physical loss." The database was deemed not "physical." The crash in that case was caused by human error during a system upgrade. The court reasoned that the risks at issue in the claim were human error or a defective program, neither of which was physical. "Unless the harm suffered, i.e., the loss of electronically stored data without loss or damage of the storage media, is determined to be a 'physical loss,' we cannot say that the risk encountered in this case, a negligent operator, constitutes a risk of direct physical loss."[29]

Other courts have concluded that data can be physical.

In Landmark American Insurance Co. v. Gulf Coast Analytical Laboratories, Inc.,[30] the insured stored its chemical analyses for customers as electronic data on a hard disk storage system. The storage system failed to read two hard disk drives, resulting in the corruption of data, in turn causing the insured to incur data recovery costs and loss of business income. The court relied on a tax case, South Central Bell Telephone Co. v. Barthelemy,[31] which concluded that electronic software data is physical.[32]

"When stored on magnetic tape, disc, or computer chip, this software, or set of instructions, is physically manifested in machine readable form by arranging

[17] No. CV 13-3728 GAF (JCx), 2013 U.S. Dist. LEXIS 152836, at *6-7 (C.D. Cal. Oct. 7, 2013).
[18] Id., at *6.
[19] Id., at *10-15.
[20] Id., at *11-14.
[21] 35 F. Supp. 3d 765 (E.D. Va. 2014), aff'd, 644 F. App'x 245 (4th Cir. 2016) (Va. law).
[22] Id. at 767.
[23] Id. at 767, 770-71.
[24] 280 F. Supp. 3d 1340 (M.D. Fla. 2017) (South Carolina law).
[25] Id. at 1343.
[26] Id., at *15-21.
[27] E.g., ISO Form No. CP 00 10 10 12 at 1.
[28] 114 Cal. App. 4th 548, 556-57 (2003).
[29] Id. at 554.
[30] No. CIV.A. 10-809 Section "B," 2012 U.S. Dist. LEXIS 45184 (M.D. La. Mar. 30, 2012).
[31] 643 So. 2d 1240, 1244 (La. 1994).
[32] Id., at *8-9.

electrons, by use of an electric current, to create either a magnetized or unmagnetized space … this machine-readable language or code is the physical manifestation of the information in binary form."[33]

The Gulf Coast court extended this reasoning to conclude that "tangibility is not a defining quality of physicality according to Louisiana law."[34] Thus, the electronic data at issue "has physical existence, takes up space on the tape, disc, or hard drive, makes physical things happen, and can be perceived by the senses."[35] The policy's "direct physical loss" requirement was, therefore, satisfied, and coverage existed.

In American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.,[36] the insured sustained a power outage, causing its three mainframe computers to lose their programming information. Even after the insured's employees reloaded the programming information, the computers could not connect to a network that tracked the insured's customers, products, and daily operations, interrupting the insured's business operations for eight hours. The insured brought the network back to operation by bypassing a malfunctioning matrix switch. Even then, however, the insured's custom configurations were lost and had to be reprogrammed. The insurer disclaimed coverage on the basis that electronic data is not physical, and that the mainframe computers and matrix switch retained their inherent abilities to be reprogrammed with the insured's custom settings, so that they were not physically damaged. The court accepted the insured's broader definition of "physical damage," reasoning that "[a]t a time when computer technology dominates our professional as well as personal lives, … 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality."[37] The court bolstered its conclusion by pointing to criminal statutes that indicated that tampering with another's computer system could cause damage.[38]

In Ashland Hospital Corp. v. Affiliated FM Insurance Co.,[39] the court predicted that Kentucky would conclude that "direct physical loss" includes heat damage that rendered a data storage less reliable. The court's discussion was scientific in nature, reviewing microscopic processes that can happen when lubricants and other components are exposed to heat, such that the loss would be deemed physical.[40]

Still other courts have relied on different policy provisions to determine whether coverage exists. For example, in Lambrecht & Associates, Inc. v. State Farm Lloyds,[41] the court based its ruling on the policy's definition of "electronic media and records" to include storage media and "data stored on such media" to conclude that loss of data due to a virus injected by a hacker was physical. In WMS Industries, Inc. v. Federal Insurance Co.,[42] the court did not reach the issue of whether loss of data could be physical. Instead, it concluded that there was no coverage because the dependent business income coverage required loss to flow from the central networked monitoring facility, whereas the loss at issue flowed from individual casinos that fed into the single, centralized jackpot.

3. MODERN CYBERLIABILITY POLICIES AND THE COVERAGE ISSUES THEY MAY PRESENT

3.1 Historical and currently available coverages[43]

The first cyber policy was introduced in 1997.[44] "Though groundbreaking as the first to address cybersecurity, it was a third-party liability policy only and was basically a 'hacker policy.'"[45]

[33] Id., at *9 (quoting Barthelemy, 643 So. 2d at 1246).
[34] Id.
[35] Id., at *10 (quoting Barthelemy, 643 So. 2d at 1246).
[36] Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. CIV 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 19, 2000).
[37] Id., at *6.
[38] Id., at *7.
[39] Civ. Action No. 11-16-DLB-EBA, 2013 U.S. Dist. LEXIS 114730, at *13 (E.D. Ky. Aug. 14, 2013) (predicting Kentucky would conclude that "direct physical loss or damage" encompassed heat damage that rendered data storage network less reliable).
[40] Id., at *13-14.
[41] 119 S.W.3d 16, 23-26 (Tex. Ct. App. 2003).
[42] 384 F. App'x 372 (5th Cir. 2010) (per curiam, unpublished opinion) (Mississippi law).
[43] Aldama & Eyerly, Cyber policies – the next wave, includes a discussion of selected provisions, terms, definitions and exclusions that may appear in some policies.
[44] Brown, B. D., 2014, "The ever-evolving nature of cyber coverage," Insurance Journal, September 22, https://bit.ly/2EncSf2.
[45] Id.

Like the electronic world, cyber policies have evolved significantly since 1997. In 2016, over 130 insurers reported writing standalone cyber policies.[46] Also in 2016, over 500 insurers provided businesses and individuals with cyber coverage, with the vast majority of those coverages written as endorsements to commercial and personal policies.[47] Cyber coverages are not written on standardized forms, and the coverages offered differ significantly.[48]

According to NAIC, the range of available coverages includes a variety of first-party and third-party coverages:

- **Liability for security or privacy breaches:** this would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- **The costs associated with a privacy breach:** such as consumer notification, customer support, and costs of providing credit monitoring services to affected consumers.
- **The costs associated with restoring, updating, or replacing business assets stored electronically.**
- **Business interruption:** including extra expense related to a security or privacy breach.
- **Liability associated with libel, slander, copyright infringement, product disparagement, or reputational damage:** this would include situations when the allegations involve a business website, social media, or print media.
- **Expenses related to cyber extortion or cyber terrorism.**
- **Coverage for expenses related to regulatory compliance:** this would include expenses incurred as a result of billing errors, physician self-referral proceedings, and Emergency Medical Treatment and Active Labor Act proceedings.[49]

Additional third-party coverages may include:

- **Liability due to breach of third parties' privacy:** such as damages based on publication, unauthorized disclosure, use, or destruction of confidential information or personally identifiable information (PII).
- **Losses due to denials or delays of access to systems:** including contingent business interruption claims. Such coverages do not typically include losses resulting from internet provider disruptions, however.
- **Losses due to transmission of malicious code or malware from the insured's affected system.**
- **Coverage for regulatory proceedings resulting from a cyber incident:** such as consumer redress funds or penalties due to payment card industry (PCI) data security standards.

The scope of available coverages seems likely to continue to evolve as the cyberworld creates new risks.

3.2 Case law involving cyberliability policies

Few cyberliability coverage cases have been decided to date. In P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.,[50] the court ruled that the cyberliability policy did not provide coverage for PCI fees assessed by credit card companies following theft of the insured's customers' credit card information.

In that case, the insured (Chang's), a restaurant, allowed its customers to pay for meals by credit card, and entered into a Master Service Agreement (Agreement) with Bank of America Merchant Services (BAMS), under which BAMS processed credit card transactions for Chang's.[51] The Agreement provided that MasterCard could assess fees against BAMS if MasterCard incurred losses from a data breach to any client of BAMS, and also contained an indemnification provision. Chang's was hacked, and the credit card numbers of over 60,000 of its customers were posted on the internet. As a result, MasterCard incurred costs for fraudulent credit card charges, for notifying customers of the breach, and for providing new credit cards and personal identification numbers. MasterCard assessed about U.S.$1.72 million in fees against BAMS, consisting of U.S.$1.7 million for fraudulent charges, and about U.S. $200,000 to issue new credit cards and related costs. BAMS sought indemnification from Chang's, which Chang's agreed to, to avoid cancellation of BAMS credit card processing services. Chang's cyber insurer disclaimed coverage, and a coverage suit ensued.

The district court ruled that no coverage existed for the U.S. $1.7 million in fees for fraudulent charges, because the policy required "injury sustained ... by a Person

[46] Insurance Journal, 2017, "Cyber insurance premium volume grew 35% to U.S.$1.3 Billion in 2016," Insurance Journal, June 23, https://bit.ly/2BVZA7R
[47] National Association of Insurance Commissioners (NAIC), 2017, "Cybersecurity," December 12, https://bit.ly/1rgyJnD
[48] Greenwald, J., 2015, "Cyber insurance policies vary widely and require close scrutiny," Business Insurance, May 10, https://bit.ly/2SWe2Hu
[49] NAIC, Cybersecurity.
[50] No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 26, 2016).
[51] Id., at *2.

because of ... unauthorized access to such Person's Record,"[52] which the court interpreted to require that the third-party claimant be the person whose confidential records had been disclosed. Because BAMS was the third-party claimant, but not the person whose records were disclosed, there was no coverage.

Although the court found that there was potential coverage for the U.S.$200,000 in fees, the exclusion "for contractual obligations an insured assumes with a third-party outside of the Policy" was held to bar coverage.[53] The court found that Chang's had voluntarily agreed to indemnify BAMS, and that there was no evidence that Chang's would have had to indemnify BAMS absent the Agreement.[54] That the Agreement is standard in the industry, that merchants cannot accept credit card payments without such agreements, and that the insurer knew this was standard practice, did not impact the court's view.[55] Instead, the court looked to the facts that the insurer and insured were sophisticated parties, and that the insured could have requested coverage for PCI fees, but did not.[56] The coverage action settled while on appeal.

4. WHAT'S NEXT?

4.1 The genuine dispute and fairly debatable doctrines as defenses to bad faith allegations

The terms of cyberliability policies are new, non-standard, and have not, for the most part, been construed by courts. The facts regarding breaches are new, with constantly evolving security measures, and with cyber tortfeasors seemingly finding new ways to get around security measures. Thus, one key question is whether the genuine dispute and fairly debatable doctrines will be viable defenses to any allegations of bad faith.

The genuine dispute doctrine is based on the insurer's "genuine dispute with its insured as to the existence of coverage liability or the amount of the insured's coverage claim."[57] Although this defense originally applied to the legal issue of policy interpretation only, some recent cases have also applied it to factual disputes.[58] A "genuine" dispute exists only where the insurer's position is "maintained in good faith and on reasonable grounds."[59] To assert this defense, the insurer must have undertaken a reasonable and proper investigation. The genuine dispute doctrine is a defense to bad faith claims only, and not to breach of contract claims.[60]

The fairly debatable doctrine, a variant of the genuine dispute doctrine, is a defense to bad faith claims where the insurer's coverage position was based on a fairly debatable interpretation and/or application of the relevant policy language.[61]

Cases decided to date suggest that these defenses remain viable. Indeed, it may be easier for insurers to rely on these defenses due to the novelty of the policies and cyber risks – assuming, of course, that the insurer has conducted the requisite coverage investigation.

In Gulf Coast, even though coverage existed for the loss, the court granted summary judgment in favor of the insurer on the bad faith claim. The court stated: "[T]here is a conflicting body of case law on [the] issue of the classification of electronic data. For that reason, there exist 'substantial, reasonable and legitimate questions to the extent of the insurer's liability' to which reasonable minds could differ and clearly do based on the case law."[62]

Retail Ventures, Inc v. National Union Fire Insurance Co. of Pittsburgh, PA[63] reached a similar result. That case was based on a claim for coverage after hackers stole the insured's customers' credit card information and used it for fraudulent transactions. Credit card companies charged the insured over U.S. $4 million for charge backs, card replacement, account monitoring, and fines. The court held that coverage existed under a computer fraud rider to a blanket crime policy, which provided coverage for "Loss which the Insured shall sustain resulting directly from: A. The theft of any Insured property by Computer Fraud."[64] However, the insurer's disclaimer did not render it liable for bad faith. First, a wrongful disclaimer is not, by itself, bad faith under Ohio law.[65] Second, the district court found that the coverage question was fairly debatable, and the fact that the disclaimer letter and claim file did not reference the "resulting directly from" language did

[52] Id., at *4-5 (emphasis added).
[53] Id., at *6, *7-8.
[54] Id., at *8-9.
[55] Id.
[56] Id.
[57] Wilson v. 21st Century Ins. Co., 42 Cal. 4th 713, 723 (2007).
[58] Id. (citing cases).
[59] Id.
[60] Id.
[61] E.g., Reid v. Pekin Ins. Co., 436 F. Supp. 2d 1002, 1013 (N.D. Iowa 2006), aff'd, 245 F. App'x 567 (8th Cir. 2007); New England Envt'l Technologies v. Am. Safety Risk Retention Group, Inc., 738 F. Supp. 2d 249, 259 (D. Mass. 2010) (no liability under Mass. Gen. L. Ch. 93A where insurer's coverage position was "based on a 'plausible interpretation' of the policy's terms").
[62] 2012 U.S. Dist. LEXIS 45184, at *13.
[63] 691 F.3d 821 (6th Cir. 2012) (Ohio law).
[64] Id. at 826.
[65] See id. at 834 (citation omitted).

not show bad faith.[66] Third, the insurer's interpretation of Exclusion 9 (which provided that "[c]overage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind") was not unreasonable because "of the confidential nature of the customer information and the claim that ejusdem generis did not apply."[67] Finally, the insurer had conducted an adequate, reasonable investigation, and requesting a second opinion from outside coverage counsel did not make "the investigation so one-sided as to constitute bad faith."[68]

These defenses may not protect insurers in all cases, however, especially in states that recognize procedural bad faith. In Travelers Property Casualty Co. of America v. Federal Recovery Services,[69] the insured, which was in the business of electronic data storage, sought coverage under a cyber errors and omissions policy for claims that it had improperly retained possession of a customer's members' account data. The court ruled that the insurer had not breached the contract, because the policy provided coverage for an "errors and omissions wrongful act," defined as "any error, omission or negligent act," but the underlying action alleged that the insured had acted knowingly, willfully, and maliciously.[70] Thus, the insurer could not be liable for substantive bad faith. However, the court ruled that the issue of procedural bad faith could proceed to trial, because the insured alleged that the insurer improperly required it to receive suit papers before making an insurance claim, and the insurer did not "diligently investigate, fairly evaluate, and promptly and reasonably communicate with" the insured, so factual disputes remained, and the fairly debatable doctrine did not allow summary judgment in favor of the insurer.[71]

An issue that may well play into the analysis of coverage under cyberliability policies is the meaning of cyber-specific terms. In BF Advance,[72] the court looked to online dictionary definitions to interpret the terms "software," "code," and "programming," which appeared in the software exclusion, but which the policy did not define. While these terms are generally understood at this time, it is possible that new meanings could develop before dictionary definitions reflect the new meanings, leading to questions about policy interpretation.

4.2 Use of conditions and exclusions as a means to promote cybersecurity

With the exception of the "no voluntary payments" condition, courts have generally been reluctant to enforce policy conditions, often requiring the insurer to prove prejudice before an insured's failure or refusal to comply can serve as a basis to disclaim coverage. For example, in Lambrecht,[73] the insurer argued, among other things, that the insured had not complied with a condition of the traditional property policy because it did not notify the police that a law might have been broken when its computer was infected by a virus. The condition at issue required the insured to "notify the police if a law may have been broken."[74] The court ruled that by its language, the condition was not a condition precedent to coverage.[75] Thus, the insurer could not disclaim coverage based on the condition.

Many cyberliability policies require the insured to maintain cybersecurity measures. A currently pending case,[76] Columbia Casualty Co. v. Cottage Health System, may provide guidance on conditions, exclusions, and the materiality of representations in policy applications, in the context of a data breach. The case is based on an alleged data breach, in which confidential medical records of the insured hospital network's patients, which were electronically stored, were disclosed to the public on the internet.[77] The "NetProtect360" policy issued to the insured contains the following condition:

[66] Id. at 834-35.
[67] Id. at 835.
[68] Id.
[69] 156 F. Supp. 3d 1330 (D. Utah 2016).
[70] Id. at 1334-1337.
[71] Id. at 1337-40.
[72] 2018 WL 4210209, at *11.
[73] 119 S.W.3d at 26.
[74] Id.
[75] Id.
[76] The federal Cottage Health matter pending when this article was originally published in 2018. It has since been voluntarily dismissed without a substantive decision on these issues. Columbia Cas. Co. v. Cottage Health Sys., No. 16-56872 (9th Cir. Jan. 26, 2018). A subsequent similar action brought in the same court also was voluntarily discontinued based on a stipulation filed on January 25, 2018. Columbia Cas. Co. v. Cottage Health Sys., No. 2:16-cv-3759, 2018 WL 1859132 (C.D.Cal. Jan. 25, 2018).
[77] Complaint for Declaratory Judgment and Reimbursement of Defense and Settlement Payments, No. 2:15-cv-03432, at ¶¶ 2-6, 16 (C.D. Cal. May 7, 2015).

Q. MINIMUM REQUIRED PRACTICES

The Insured warrants, as a condition precedent to coverage under this Policy, that it shall:

1. follow the Minimum Required Practices that are listed in the Minimum Required Practices endorsement as a condition of coverage under this policy, and

2. maintain all risk controls identified in the Insured's Application and any supplemental information provided by the Insured in conjunction with Insured's Application for this Policy.[78]

Perhaps because conditions can be difficult to enforce, some cyberliability policies also exclude coverage if the insured has not taken cybersecurity measures. The declaratory relief complaint filed in Cottage Health System[79] alleges that the "NetProtect360" policy also contains the following exclusion:

Whether in connection with any First Party Coverage or any Liability Coverage, the Insurer shall not be liable to pay any Loss:

***

O. FAILURE TO FOLLOW MINIMUM REQUIRED PRACTICES BASED UPON, DIRECTLY OR INDIRECTLY ARISING OUT OF, OR IN ANY WAY INVOLVING:

1. Any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing;...

The policy also contains a condition incorporating the application, which contains numerous questions regarding cybersecurity, and making the insured's representations in the application material to the risk.[80] California law provides ample guidance on misrepresentations in applications for other types of policies,[81] although Cottage Health could provide guidance on such provisions specifically in the cyberliability policy context.

The policy at issue in Cottage Health contains a provision requiring ADR before any judicial proceeding is filed, prompting the district court to dismiss the complaint without prejudice,[82] and the appeal was voluntarily dismissed.[83] The insured then filed a complaint in state court,[84] where the case now appears to be headed for trial in the late summer or fall of 2019.[85] so it is possible that insurers and insureds will ultimately obtain some guidance regarding the enforceability of the exclusions and/or conditions at issue in Cottage Health.

Forensic investigation of alleged cyber losses[86] could also become an area for dispute, placing cooperation conditions and claims handling at issue. Causation of the alleged loss may be key to evaluating coverage, as the policy provisions quoted in this article indicate. In Southwest Mental Health Center, Inc. v. Pacific Insurance Co.,[87] the insurer made a spoliation argument, seeking to exclude evidence regarding the insured's computer itself in a coverage action, because one of the insured's employees had discarded the damaged drive a year after the loss. The court found that there was no spoliation because the insurer did not request the drive for inspection during that year, the insured discarded it as part of its "routine clean-up," and there was no indication that the insured had done so in an effort to prevent the insurer from determining the cause of damage.[88]

5. CONCLUSION

Given the wide variety of policies on the market and the ingenuity of cyber villains, insureds are well advised to select and negotiate their cyberliability policies carefully, based on an analysis of their specific needs and the specific risks to which they are exposed. Insurers may wish to carefully investigate cyberliability coverage claims, keeping in mind that the cyber landscape will likely continue to develop rapidly.

[78] Id., at ¶ 27.
[79] Id., at ¶ 26.
[80] Id., at ¶¶ 27, 29-31.
[81] E.g., Williamson & Vollmer Engineering, Inc. v. Sequoia Ins. Co., 64 Cal. App. 3d 261, 274-275 (1976).
[82] Columbia Cas. Co. v. Cottage Health Sys., No. 2:15-cv-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. July 17, 2015).
[83] Columbia Cas. Co. v. Cottage Health Sys., No. 16-56872 (9th Cir. Jan. 26, 2018).
[84] Cottage Health Sys. v. Columbia Cas. Co., et al., No. 16CV02310, Santa Barbara, California Superior Court, Complaint (filed May 31, 2016).
[85] Id., Docket, at 8 (reviewed Feb. 23, 2019).
[86] See Seals, T., 2015, "ISACA lays out forensics in the data breach era," Infosecurity Magazine, March 24, https://bit.ly/2tve9u7
[87] 439 F. Supp. 2d 831, 840 (W.D. Tenn. 2006).
[88] Id.

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO