CYBER POLICIES—THE NEXT WAVE

ABA Insurance Coverage Litigation Committee CLE Seminar
Tucson, Arizona | March 1, 2018

Karin S. Aldama
Perkins Coie LLP
2901 N. Central Avenue, Suite 2000
Phoenix, AZ 85012-2788
Telephone: (602) 351-8270
Facsimile: (602) 648-7172
www.perkinscoie.com
kaldama@perkinscoie.com

Tred R. Eyerly
Damon Key Leong Kupchak Hastert
1600 Pauahi Tower
1003 Bishop Street
Honolulu, HI 96813
Telephone: (808) 526-3625
Facsimile: (808) 533-2242!
www.hawaiilawyer.com
te@hawaiilawyer.com
Blog: insurancelawhawaii.com

1. Overview of the Issues

Coverage for cybersecurity is still in its infancy. This is problematic because brokers tend to be unfamiliar with the various potential coverages available and with the overall insurance needs of their varied clients. Despite widely publicized cyberattacks, many businesses remain unaware of the risks of, and the cost associated with responding to, a cyberattack.

Even law firms are behind the curve in being adequately covered for cyberattacks. An American Bar Association study recently found that 77 percent of responding firms did not have cyber insurance, 95 percent of responding firms were noncompliant with their own cyber policies, 100 percent were noncompliant with a client's policies, and 53 percent of responding firms did not have a data breach incident response plan.[1]

Insureds may argue that traditional first-party property and commercial general liability ("CGL") policies provide some coverage. Such arguments have met with some success, but many cases have determined that losses related to data do not meet these policies' requirements of a direct *physical* loss of *tangible* property.[2] Moreover, in May 2014, the Insurance Services Office, Inc. ("ISO") issued endorsements for use with CGL policies designed to clarify that traditional CGL policies do not provide cyber coverage.[3]

In addressing various issues associated with cyber coverage, this article first looks at insureds' arguments for coverage under a variety of traditional policies and insurers' responses to those arguments, as well as courts' resolutions of the issues presented. It then discusses the ongoing evolution of cyber policies, as well as important features of currently available cyber policies and how some of the initial cases starting to address actual cyber policies (as opposed to more traditional policies under which cyber coverage has been sought) have treated those policies. Finally, the article discusses how, in the likely "next wave" of issues to arise with respect to cyber coverage, arbitrators or courts may evaluate insureds' allegations of bad faith if insurers disclaim coverage for claims under cyber policies. With no standard language and little published guidance on interpreting cyber policies, what standards should be applied to evaluate coverage disputes, including claims of bad faith?

---

[1] ABA Journal, How Prepared are Law Firms for Cyber Breaches? And How Often are Firms Being Attacked? (June 29, 2017 8:41 AM (available at http://www.abajournal.com/news/article/how_prepared_are_law_firms_for_cyber_breaches_and_how_often_are_they_being_).

[2] *E.g., Seagate Tech., Inc. v. St. Paul Fire and Marine Ins. Co.*, 11 F. Supp. 2d 1150 (N.D. Cal. 1998); *Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co.*, 114 Cal. App. 4th 548 (Cal. Ct. App. 2003).

[3] *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INSURANCE JOURNAL (July 18, 2014), (commenting on forms CG 21 06 05 14 and CG 21 07 05 14) (available at https://www.insurancejournal.com/news/east/2014/07/18/332655.htm).

a. Initial Coverage Under Traditional Policies

Coverage for cyber-related issues dates back 20 or 25 years.[4] Arguably, property and liability policies could provide coverage for loss due to cyberattacks for the following types of claims:

- Business interruption
- Loss of income
- Cost of extortion
- Intangible property: costs to restore or recreate data or software
- Notifying customers or clients of breach
- Hiring lawyers and public relations firm
- Establishing call-in centers for affected customers or clients
- Forensic costs of investigating a cyber attack[5]

But property policies typically require "direct physical loss."[6] Thus, insurers have, at times successfully, taken the position that cyberattacks did not implicate a physical loss.[7] Other courts have come to different conclusions.[8]

Similarly, most CGL policies provide coverage for "property damage," and define that term to require tangible property.[9] Since 2004, the main ISO CGL form has specified that "electronic data is not tangible property."[10] As noted above, optional ISO endorsements contain exclusions for cyber risks under CGL exclusions.[11] But even with respect to older CGL policies that do not contain these definitions and endorsements, it is by no means clear that losses relating from cyber breaches will be covered.[12]

Before cyber policies were available, technology companies relied upon traditional errors and omissions ("E&O") policies to cover various liabilities faced by the industry. This included such risks as a software product malfunctioning and affecting a customer's network, unauthorized

---

[4] Brian D. Brown, *The Ever-Evolving Nature of Cyber Coverage*, INSURANCE JOURNAL, Sept. 22, 2014 (available at https://insurancejournal.com/magazines/features/2014/09/22/340633.htm (hereinafter "Brown Article")).

[5] Jason Cieri, *I've Been Hacked? Am I Covered?*, Merlin Law Group Prop. Ins. Coverage Law Blog (Oct. 10, 2017) (available at http://www.property insurancecoveragelaw.com/2017/10/articles/insurance/ive-been-hacked-am-i-covered/).

[6] *E.g.*, ISO Form No. CP 00 10 10 12 at 1.

[7] *E.g.*, *Ward Gen. Ins. Servs., Inc.,* 114 Cal. App. 4th at 556-57 (no coverage for database crash, as database was not "physical").

[8] *E.g.*, *Ashland Hosp. Corp. v. Affiliated FM Ins. Co*., 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).

[9] *E.g.*, ISO Form No. CG 00 01 04 13 at 15.

[10] ISO Form Nos. CG 00 01 12 04 at 15, CG 00 01 12 07 at 15, CG 00 01 04 13 at 15.

[11] Ron Biederman, *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INSURANCE JOURNAL (July 18, 2014) (available at https://www.insurancejournal.com/news/east/2014/07/18/332655.htm (commenting on forms CG 21 06 05 14 and CG 21 07 05 14)).

[12] *See., e.g., Seagate Tech., Inc.*, 11 F. Supp. 2d at 1153-54 (Cal. law) (loss of customer's information due to disk drive failure was not "physical damage to tangible property"); *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 93-98 (4th Cir. 2003) (Va. law) (loss of stored data after installing insured's defective software not loss of tangible property).

access to a client's system, destruction of data, or a virus attack. Coverage for these incidents was frequently added by endorsement to the E&O policy. The endorsements were eventually expanded to provide coverage for breaches of confidential information.[13] Still, it became apparent that some companies holding considerable amounts of confidential consumer information were not adequately covered by E&O policies. Instead, these companies needed standalone cyber policies that would cover network security and privacy liability.[14]

But even with the more recent advent of cyber policies, maintaining and utilizing traditional forms of coverage remains important for cyber-related risks. Shareholders expect that good corporate governance and oversight include safeguarding a company's cyber-systems and data. D&O policies may come into play where class-action suits allege that "wrongful act[s]" taken by a company's board or officers allowed cyberattacks to occur—which "wrongful act[s]" could be covered by D&O policies. Therefore, business and corporate policyholders need to preserve responsive D&O coverage for potential cyber claims that could be brought against senior executives.[15] Further, E&O policies may be available to respond to allegations of a company's errors or omissions in rendering its professional services, which, in turn, caused cyber incidents, or allowed them to occur. [16]

Businesses have also attempted to use crime policies to obtain coverage for some forms of cyberattacks, particularly ones related to phishing schemes and social engineering fraud. These attempts, too, have met with mixed success. Courts often find that there is no coverage for losses resulting from these types of attacks because the losses do not "result directly" from the use of a computer, as required by the policies, but rather require human intervention.[17] But there are some cases that reach a contrary result, sometimes specifically rejecting the reasoning of courts finding insufficient direct causation.[18] Overall, however, crime policies, like the other policies discussed above, do not provide solid protection against the risk of losses from cyberattacks—they at best can supplement cyber policies.

In summary, while CGL, D&O, E&O, and crime policies may be sources of coverage for some cyber-related losses, exclusions or other provisions in those policies are often interpreted to

---

[13] Laura Floresca, *Cyber Insurance 101: The Basics of Cyber Coverage*, Woodruff Sawyer & Co. Blog, Cyber Noteook (June 19, 2014) (available at https://wsandco.com/cyber-liability/cyber-basics/ (hereinafter, "Floresca Article")).

[14] *Id.*

[15] Cort T. Malone and Jorge R. Aviles, *Swipe Right on Insurance: Risks and Coverage Implications for Mobile Apps and Social Media Platforms*, ANDERSON KILL (Oct. 26, 2017) (available at https://www.andersonkill.com/Publication-Details/PublicationId/1562).

[16] *Id.*

[17] *E.g.*, *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252, 258-59 (5th Cir. 2016) (holding that there was no coverage for loss from social engineering fraud because "the transfers were made not because of fraudulent information, but because [the insured] elected to pay legitimate invoices," albeit to a fraudulent bank account; that is, "the invoices, not the [fraudulent] email, were the reason for the funds transfers") (per curiam, unpublished opinion) (Tex. law).

[18] *E.g.*, *Medidate Sols., Inc. v. Fed. Ins. Co.*, No. 1:15-cv-00907-ALC (S.D.N.Y. July 21, 2017) (granting summary judgment to insured under crime policy for $4.7 million loss resulting from social engineering fraud; specifically rejecting *Apache's* finding of insufficient direct causation by stating that "the Court finds [*Apache*'s] causation analysis unpersuasive" and holding that the insured's "employees only initiated the transfer as a direct cause of the thief sending spoof[ed] emails" with fraudulent transfer instructions).

bar coverage for cyber-related events. Insureds, risk managers, and brokers need to be aware of the evolving case law and exclusions, and well as of developments in the area of cyber-specific policies, if they wish to maximize coverage and avoid coverage gaps that exclusions or judicial interpretations of policy language may create.

b. Evolution of Cyber Policies

The first cyber policies appeared in the late 1990s. These were liability policies that covered third-party suits arising from breaches originating outside the company. Loss caused by rogue and disgruntled employees was often excluded as constituting acts deemed malicious. Policy language narrowed coverage by defining employees as "any individual whose labor or service is engaged by and directed by the insured." Consequently, an employee acting outside the scope of employment to breach an internal system would not be an insured under the policy, and no coverage would be afforded.[19]

The initial cyber policies also had other exclusions, including ones for responding to regulatory inquiries and for fines and penalties resulting from such inquiries. Further, little, if any, first-party coverage was offered.[20]

Network extortion became prominent in the early 2000s. This included using stolen data to threaten a company's reputation or corrupting data on a company's network. Consequently, a separate insuring agreement was created to address extortion resulting from a network attack.[21]

At the same time, state laws were enacted to protect the privacy of companies and individuals from cyber threats, causing a change in coverage. Most states followed California's 2003 lead by enacting security breach information laws requiring a business or agency to notify affected individuals of any data breach if personally identifiable information ("PII") was accessed by an unauthorized person. PII under these statutes included individuals' first or last name in combination with a social security number, drivers' license number, or account, credit or debit card numbers in connection with an access code or password.[22] The enactment of these statutes resulted in a need for new policies.

Cyber policies are not written on standard forms, and the coverages provided have varied widely.[23] Types of coverages offered now include, as discussed in more detail below, both first-party and third-party coverage for various costs and losses related to different cyber incidents such as data breaches, unauthorized disclosure of PII, cyber extortion, ransomware, and denial or delay of service attacks.

---

[19] Brown Article.

[20] Prowriters, *The History of Cyber Insurance (*April 25, 2016) (available at http://prowritersins.com/download/The-History-of-Cyber-Insurance-041316V1.pdf (hereinafter "Prowriters Article")).

[21] Brown Article.

[22] *Id.*

[23] Judy Greenwald, *Cyber insurance policies vary widely and require close scrutiny*, Business Insurance (May 10, 2015 12:00 AM) ("There are about 40 to 50 insurers that offer multiple products – all different …") (available at http://www.businessinsurance.com/article/00010101/NEWS06/305109992/Cyber-insurance-policies-vary-widely-and-require-close-scrutiny (hereinafter "Greenwald Article")).

Historically, most of the losses paid through cyber policies have been for costs incurred in complying with state notification laws (particularly because a single breach may, depending on its geographical reach, require compliance with the notification requirements of several states). Paid losses have also included the cost to investigate and respond to breaches or potential breaches, such as costs for computer forensics, legal representation, and public relations expenses. And there have been paid losses for fines and penalties.[24]

But cyber policies continue to evolve, and insurers have changing attitudes in what and how much they are willing to cover. Larger insurers are better able to provide coverage than insurers with a small market share. Pricing for cyber policies is still volatile and coverage differs from policy to policy.[25]

Consequently, even today there is little standardization, making direct comparisons among carriers' policies difficult.[26] Forms are still in flux. And analyzing cyber coverage is all the more difficult due to the ever-evolving nature of the threats and attack methods, and to rapid technology changes such as smart phones and tablets.

2. Coverage Cyber Losses Under Non-Cyber Policies Addressed in Court

While there has been litigation regarding data breaches, few published cases have specifically addressed cyber policies. Rather, the body of existing case law has generally developed under non-cyber policies such as CGL, property, commercial crime and D&O policies.[27]

This is changing to some extent as disputes under actual cyber policies are slowly making their ways into courts. But cyber policies may contain ADR provisions that will hinder the development of case law specifically interpreting their language. For example, one recently issued cyber policy provided, as summarized by the court:

> "All disputes and differences between the Insured and the Insurer which may arise under or in connection with this policy . . . shall be submitted to the alternative dispute resolution ("ADR") process" and that if mediation is the chosen method of ADR "no . . . judicial proceeding shall be commenced until the mediation shall have been terminated and at least 60 days shall have elapsed from the date of the termination . . . ."[28]

The remainder of this section summarizes the development of cyber-related case law under traditional, non-cyber policies.

---

[24] *Id.*

[25] Prowriters Article.

[26] Greenwald Article.

[27] Many of the cases discussed below are collected in an article entitled, "Cybersecurity – Liability Developments And Insurance Coverage For The Risks And Losses," by Scott Godes and Alexander Barnstead, Barnes & Thornburg, LLP.

[28] *Columbia Cas. Co. v. Cottage Health Sys*., No. CV 15-03432 DDP (AGRx), 2015 U.S. Dist. LEXIS 93456, at *1-2 (C.D. Cal. July 17, 2015).

a. Results Under Traditional First-Party Property Policies

An early case under a first-party property policy involved damage to the policyholder's computer systems as a result of a power outage.[29] The policy provided coverage for "direct physical loss or damage." The insurer disclaimed coverage because electronic data is not "physical," and the mainframe computer and matrix switch at issue retained their inherent abilities to be reprogrammed with the insured's custom settings, so that they were not physically damaged. The court ruled, however, that the loss of custom settings to the mainframe was "direct physical loss or damage" under a first-party policy.[30] The court used the thin rationale that in this day and age "computer technology dominates our professional as well as personal lives," justifying the insured's broader interpretation of "direct physical loss or damage"; moreover federal and other states' penal laws made it a criminal offense to cause damage to another's computer system.[31]

Likewise, in *Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs*, a hard drive failure led to corruption of data, and the insurer denied coverage under a property policy.[32] The court disagreed because the "electronic data 'has physical existence, takes up space on the tape, disc, or hard drive, makes physical things happen, and can be perceived by the senses.'"[33]

In *Lambrecht & Assocs. v. State Farm Lloyds*, the insured's computer system was infected by a virus, giving rise to a claim for lost business income, the costs of replacing the server and software packages, and the costs of hiring someone to input data into the new systems.[34] The policy at issue provided coverage for "accidental direct physical loss," but excluded coverage for, as summarized by the court,

> "any loss of 'business income' caused by accidental direct physical loss to 'electronic media and records' after the longer of" sixty consecutive days from the date of the loss or the amount of time necessary to repair, rebuild or replace other property at the premises caused by the same occurrence.[35]

The insurer disclaimed coverage, and, in the subsequent coverage action, argued that the losses were not "physical" because they were not "tangible."[36] The court aptly summarized and then sidestepped this challenging issue, stating:

> Most of these opinions [such as *Ingram Micro*] focus on the physical nature of the data itself and debate whether or not it can be dissolved into a quantitative mass or is entirely transcendental. We need not attempt to compose such an erudite thesis because the issue of whether or not the losses

[29] *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. CIV 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (Ariz. Law).
[30] *Id*., at * 4.
[31] *Id*., at *6.
[32] No. CIV.A. 10-809 Section "B," 2012 U.S. Dist. LEXIS 45184 (M.D. La. Mar. 30, 2012) (La. law).
[33] *Id*., at *4 (citation omitted).
[34] 119 S.W. 3d 16 (Tex. Ct. App. 2003).
[35] *Id*. at 24.
[36] *Id*. at 23-24.

> alleged by [the insured] are covered by the policy can be determined by analyzing the policy itself.[37]

Because the policy defined "electronic media and records" to include storage media and "data stored on such media," the alleged loss was "physical" within the plain meaning of the policy as a matter of law.[38] Moreover, the court ruled that the loss was accidental because there was no evidence that the insured could have reasonably anticipated the resulting damage to its computer system caused by the hacker.[39]

On the other hand, in *Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co.*, the court found there was no coverage for a database crash because there was no "direct physical loss."[40] The court reasoned, "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 cases, a negligent operator, constitutes a risk of direct physical loss."[41]

Some decisions have been based on different policy provisions. In *WMS Indus., Inc. v. Fed. Ins. Co.*, the insured supplied networked slot machine systems to various casinos.[42] The slot machines were part of a single progressive jackpot, with bets paid into a central monitoring location and winnings paid from that location. The network was interrupted during Hurricane Katrina, due to physical damage to one of the central monitoring facilities. Coverage existed under the policy's dependent business premises coverage, but the amount of losses exceeded the low limits for that coverage, and the insured sought coverage under the business income and extra expense ("BI/EE") coverage, which had much higher limits. The court ruled that there was no BI/EE coverage, because the policy required BI/EE loss to flow from the central monitoring facility, but here, that loss flowed from the individual casinos.[43]

b. Results Under Traditional CGL Policies

Coverage was denied under a third-party liability policy for the manufacturer of disk drives for personal computers in *Seagate Tech., Inc. v. St. Paul Fire and Marine Ins. Co*.[44] Amstrad, a manufacturer of personal computers, sued Seagate, alleging that the disk drives were failing. Seagate's policy provided liability coverage for "physical damage to tangible property of others."[45] While the underlying complaint alleged "loss of customer's information," it did not suggest that components of the host computer, other than the Seagate's drives, suffered damage.[46] Consequently, the loss of data, by itself, was not "physical damage to tangible property" under the policy.[47]

---

[37] *Id*. at 24-25.
[38] *Id*. at 24-26.
[39] *Id*. at 23.
[40] 114 Cal. App. 4th 548 (Cal. Ct. App. 2003).
[41] *Id*. at 554.
[42] 384 F. App'x 372 (5th Cir. 2010) (per curiam, unpublished opinion) (Miss. law).
[43] *Id*. at 375.
[44] 11 F. Supp. 2d 1150 (N.D. Cal. 1998) (Cal. law).
[45] *Id*. at 1153.
[46] *Id*. at 1155.
[47] *Id*. at 1154.

Although it did not involve hacking, another early case from the Fourth Circuit demonstrates the problems insureds may confront in seeking coverage under a CGL policy when seeking to obtain coverage for IT-related losses.[48] After AOL released its Version 5.0 access software, it was sued in numerous class actions alleging that the software had substantial bugs and was incompatible with the plaintiffs' other applications software and operating systems, causing the computers to be damaged. Specifically, the plaintiffs alleged "that Version 5.0 altered the plaintiffs' existing software, disrupted their network connections, caused the loss of stored data, and caused their operating systems to crash."[49] The insurer denied coverage because the claimed damages were not to tangible property, as required by the policy's definition of "property damage," and also fell under the impaired property exclusion.[50] The Fourth Circuit affirmed summary judgment in favor of the insurer, distinguishing between the physical components of computers and data. The court explained:

> The … policy … covers liability for "physical damage to tangible property," not damage to data and software, i.e., the abstract ideas, logic, instructions, and information. Thus, while it covers any damage that may have been caused to circuits, switches, drives, and any other physical components of the computer, it does not cover the loss of instructions to configure the switches or the loss of data stored magnetically. These instructions, data, and information are abstract and intangible, and damage to them is not physical damage to tangible property.[51]

Other cases have involved CGL Coverage B for personal (or reputational) injury. A defense was found owing under a non-standard CGL policy when patient records were placed on the internet and made searchable.[52] Two policy periods were at issue, and they provided coverage for, as summarized by the court, "injury arising from (1) the 'electronic publication of material that . . . gives unreasonable publicity to a person's private life' (the language found in the 2012 Policy) or (2) the 'electronic publication of material that . . . discloses information about a person's private life' (the language found in the 2013 Policy)."[53] The court found that there was a publication because "exposing confidential medical records to public online searching placed highly sensitive, personal information before the public."[54] Consequently, the insurer had a duty to defend.[55]

A similar result was reached in *Hartford Cas. Ins. Co. v. Corcino & Assocs*., where the court implicitly concluded that the posting of the insured hospital's patient data on a public website was a "publication" under the CGL policy.[56] There, the insurer did not dispute that the underlying actions involved claims that the insured was liable for electronic publication of material that

---

[48] *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003) (Va. law).
[49] *Id*. at 91-92.
[50] *Id.* at 92.
[51] *Id.* at 96.
[52] *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC*, 35 F. Supp. 3d 765 (E.D. Va. 2014), *aff'd*, 644 F. App'x 245 (4th Cir. 2016) (Va. Law).
[53] *Id.* at 767.
[54] *Id.* at 769.
[55] *Id.* at 772.
[56] No. CV 13-3728 GAF (JCx), 2013 U.S. Dist. LEXIS 152836, at *6-7 (C.D. Cal. Oct. 7, 2013).

violated the underlying plaintiffs' rights of privacy, but there was an issue as to whether an exclusion nonetheless precluded coverage.[57] The court found that the 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" did not bar coverage because the underlying plaintiffs sought relief under the state constitution and common law, and an exception to the exclusion for "liability for damages that the insured would have in absence of such state or federal act" reinstated coverage.[58] The court reasoned that the fact that the plaintiffs also sought relief under two statutes did not change the result because those statutes did not create new rights of privacy, but rather merely codified existing law.[59]

In *Innovak Int'l, Inc. v. Hanover Ins. Co.*, on the other hand, the court found that there was no coverage under Coverage B of a CGL policy because the underlying plaintiffs did not allege publication of their personal private information, but appropriation of their information by third-party hackers.[60] The insured argued that the underlying plaintiffs had alleged that the insured had published software, rather than the plaintiffs' private information, but the court found that publication of the insured's software did not violate the underlying plaintiffs' right of privacy, as required for coverage to be available under Coverage B.[61]

c. Results Under Crime Policies

Coverage under a crime policy was considered in *Retail Ventures, Inc v. National Union Fire Insurance Co. of Pittsburgh, PA*, where hackers had been able to view credit card information of the insured's customers, and had used that information for fraudulent transactions.[62] Credit card companies charged the insured over $4 million for costs for charge backs, card replacement, account monitoring, and fines.[63] The court ruled there was coverage under a computer fraud rider to the blanket crime policy for amounts owed to the credit card companies, where the policy provided coverage for " Loss which the Insured shall sustain resulting directly from: A. The theft of any Insured property by Computer Fraud."[64]

The *Retail Ventures* court also ruled that Exclusion 9, which provided: "Coverage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind," did not bar coverage.[65] It based that finding on its conclusion that the credit card information at issue was not proprietary information because it was "owned or held by many, including the customer, the financial institution, and the merchants to whom the information is provided in the ordinary stream of commerce."[66] Interpreting "other confidential information of any kind" to mean "any information belonging to anyone that is

---

[57] *Id*., at *7.
[58] *Id*., at *6-7.
[59] *Id*., at *11-14.
[60] No. 8:16-cv-2453-MSS-JSS, 2017 U.S. Dist. LEXIS 191271 (M.D. Fla. Nov. 17, 2017) (S.C. law).
[61] *Id*., at *15.
[62] 691 F.3d 821 (6th Cir. 2012) (Ohio law).
[63] *Id*. at 824.
[64] *Id*. at 826. In reaching this conclusion, the court also affirmed the district court's prediction that Ohio state courts would apply a proximate cause standard to determine whether the loss "result[ed] directly" from the covered peril. *Id*. at 831-32.
[65] *Id*. at 832.
[66] *Id*. at 833.

expected to be protected from unauthorized disclosure" would render the other terms in the exclusion meaningless and eviscerate coverage for computer fraud.[67]

In another crime policy case, the court concluded that human error, not computer fraud, caused the insured's loss.[68] In that case, the policyholder was defrauded into sending money to a criminal instead of its vendor, after receiving spoofed telephone calls and an email instructing the insured to use new bank account information for routing payments. The email, sent from a fraudulently created account with a different domain name than the vendor's, attached a letter on the vendor's letterhead with bank account information, and stated a copy would follow by traditional mail. After a minimal investigation, the insured's employees changed the bank routing information to the fraudulent account.[69]

When the vendor asked about the status of payment, the insured learned that it had been defrauded and sought coverage under its commercial crime policy. The relevant Computer Fraud provision of the insured's crime policy stated:

> We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or
>
> b. to a place outside those premises.[70]

The insurer disclaimed coverage because the "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds."[71] While the district court found there was coverage despite human intervention causing the error, the Fifth Circuit reversed. Although an email was part of the scheme, it was merely incidental to the occurrence of the authorized transfer of money by the insured.[72] For example, employees had called the fake number in the emailed letter to confirm the new bank information, employees had authorized the new payment instructions, and employees had "elected to pay legitimate invoices" to the wrong bank account.[73]

In a similar case, summary judgment was granted under a crime policy after the insured law firm followed email instructions to accept a check from the debtor and wire the amount in the check, less the firm's fee, to the alleged overseas client.[74] The law firm subsequently learned that the initial check was fraudulent, and submitted a claim to Travelers because all of the communications had been through emails and via computers, triggering coverage under the crime

---

[67] *Id*.
[68] *Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016) (per curiam, unpublished opinion).
[69] *Id.* at 253.
[70] *Id*. at 254.
[71] *Id.*
[72] *Id.* at 258.
[73] *Id.* at 258-59.
[74] *Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 095024601S, 2011 Conn. Super. LEXIS 1572 (Conn. Super. Ct. June 24, 2011).

policy. Travelers denied the claim on the basis that it did not involve computer fraud, and that the alleged loss was not directly caused by computer fraud. On summary judgment, the court reasoned that the overseas client communicated with the law firm by email and the fraudulent check may have been created by the use of a computer.[75] Moreover, it found the policy be ambiguous as to the amount of computer usage necessary to constitute computer fraud, and, for those reasons, granted summary judgment for the insured.[76]

d. Result Under an E&O Policy

In *Eyeblaster, Inc. v. Federal Insurance Co.*, the insured was sued by a computer user, alleging his computer, software and data was injured after he visited the insured's website.[77] Eyeblaster, the insured, tendered a claim to Federal Insurance Company under its General Liability and E&O policies. Federal denied a defense and prevailed on its summary judgment motion in the district court, but the Eighth Circuit reversed.[78] On appeal, Federal argued the underlying complaint did not allege a "wrongful act," but rather alleged merely that Eyeblaster had acted intentionally by installing tracking cookies, Flash technology, and JavaScript on the customer's computer, all of which were intentional acts.[79] But the court found that Federal could point to no evidence that doing so was intentionally wrongful.[80] Moreover, Federal also had not carried its burden to show intentional conduct, which also precluded summary judgment in its favor.[81]

3. Currently Available Cyber Coverage

a. Overview of Cyber Policies

The number of insurers that provide cyber coverage, and the product they offer, is increasing. But there is not yet any "standard form" cyber coverage. At the same time, the era of entirely manuscript policies are gone. Instead, insurers are creating their own standard policy forms, with coverage that can differ significantly from "standard" form to "standard" form. Differences in coverage offered by various insurers include first- versus third-party coverage (or both), the types of covered losses, the scope of coverage for certain losses, whether the insurer provides consultancy services in case of a data breach, and the type and scope of exclusions.

Whatever the "standard" form provided by an individual insurer, that form can typically be modified to some extent in negotiations during the underwriting process. How significant the modifications that an insurer is willing to make depends, as always, at least to some extent on the policyholder's willingness to pay additional premiums.

Having said that, there are certain features of cyber policies that are commonly relevant when cyber issues arise, so that the availability or inclusion of such features in a cyber policy (or the lack thereof) should be taken into consideration when determining which of the currently

[75] *Id.*, 2011 Conn. Super. LEXIS 1572 at *25.
[76] *Id.*
[77] 613 F.3d 797 (8th Cir. 2010) (Minn. law).
[78] *Id.* at 799.
[79] *Id.* at 804.
[80] *Id.*
[81] *Id.* at 804-05.

available cyber policies to choose and which modifications to seek. One of the most basic such features is whether a policy provides first-party or third-party coverage, or both. Once that is determined, there are other policy provisions—such as definitions, exclusions, types of coverage provided, and warranties—that should be considered in the underwriting process. This section addresses these issues.

b. First- versus Third-Party Coverage

As do many types of policies, cyber policies distinguish between first-party and third-party coverage. Some cyber policies provide one or the other type of coverage, some provide both. The type of exposure faced by any given policyholder typically determines what coverage it should seek.

First-party cyber policies provide coverage for cyber-incident-related losses experienced by the insured itself. Typical coverages are for:

- Data asset protection, that is the restoration or replacement of lost or damaged data. This type of coverage can also be helpful with respect to lost or damaged software, particularly custom-built software.

- Remediation costs associated with a cyber incident. Those costs can include the costs of notifying customers or other third parties in accordance with applicable state and federal laws, the costs of forensic investigations into the origin and cause of the incident, and legal costs associated with the above.

- Business interruption coverage for interruption to the affected business itself through, for example, a denial-of-service attack in which access to, e.g., an on-line vendor's network is blocked, preventing customers from making purchases.

- Cyber extortion coverage. This type of coverage typically pays for costs associated with a cyber extortion or ransomware attack, in which the affected business' data is encrypted by malware and will supposedly (but not always) be decrypted upon payment of a ransom, generally in an electronic currency such as BitCoin. Cyber extortion can also involve threats of denial-of-service or similar attacks, with payments to the extortionist required in order to avoid the attack. Costs associated with cyber extortion typically consist of the potential ransom itself; costs associated with negotiating and paying the ransom (such as the retention of consultants to conduct the negotiations, or out-of-state travel costs to pay the ransom); and, in case of ransomware attacks, the replacement or restoration of the affected data if the ransom is not paid or the encryption is not reversed even with payment (which is not an infrequent occurrence).

- Crisis management and other response costs, such as costs for PR firms to handle communications with customers and the public, costs for credit monitoring that may be required in situations where customers' credit card information has been hacked, or the costs for setting up and operating crisis management centers to allow potentially affected individuals to get information about the cyber incident and their risk exposure.

Third-party policies, on the other hand, provide coverage for the insured's liability to third parties that result from a cyber event. Generally covered losses include:

- Losses incurred by, or damages payable to, third parties for the unauthorized disclosure, use, or destruction of their confidential information or of PII. Notably, this coverage is broader than the hacking of credit card or social security numbers that typically comes to mind. While losses resulting from the disclosure of such PII would be covered under a third-party policy, the coverage can also extend to information that is "merely" confidential, but does not fit the stringent definition of PII. Such confidential information can include, e.g., proprietary business information of an affected business' customers or vendors, or client information held by law firms.

- Losses incurred by third parties because of denials or delays of access to the affected business' systems, including business interruption losses incurred by the affected business' vendors or customers. Third-party coverage typically does not, however, cover losses resulting from internet service provider disruptions.

- Losses incurred by third parties that result from the transmission of malicious code or malware from the affected business' systems.

- Damages payable by the affected business to third parties because of copyright infringement, misappropriation of trade secrets, defamation, or invasion of privacy if caused by, e.g., data hacked from the affected business' systems. Notably, third-party coverage generally does not pay for losses associated with allegations of patent or trade secret infringement, even though misappropriation and copyright infringement are covered.

- Defense costs in any legal proceeding against the affected business instituted by a damaged third party.

- Costs associated with regulatory proceedings, including both legal costs and the costs of fines or sanctions, resulting from a cyber incident. These costs can include, e.g., consumer redress funds or penalties due to Payment Card Industry ("PCI") Data Security Standards.

As always, appropriate coverage, including appropriate limits and retentions, should be selected based on any given client's or business' business model. For example, a business that retains a lot of third-party confidential data on its systems should seek higher third-party coverage limits for potential cyberattacks thereon, whereas an on-line vendor may also want to focus on first-party business interruption coverage. The important take-away is that there are different options available, and that any given policy should be tailored to the insured, if necessary through negotiations and endorsements.

c. Important Policy Provisions and Fine Print

In the continued absence of standardized forms for cyber policies, policies offered by different insurers continue to vary as to the terms, endorsements, exclusions, and conditions they offer. That makes it, if anything, even more important than normal for policyholders seeking coverage to assess and compare the details of all offered policies, and to select coverage (and request endorsements, if necessary) to fit their particular needs, exposures, and business model. This section discusses some of the most relevant common policy provisions and their potential impacts on available coverage.

i. Definition of Data

For any policy covering data restoration or replacement, the definition of "data" is key. It typically includes PII, but should also include the type of non-PII confidential data discussed above—trade secrets, proprietary business information, and other confidential non-PII information a particular business routinely handles. Importantly, "data" should include data of the policyholder's employees, as HR departments virtually always have access to both PII and confidential employee data. Also, consider whether "data" should include non-electronic data—whether it should depends on coverage provided by the policyholder's other policies.

ii. Definition and Scope of Covered Losses

What constitutes a "loss" is also key to defining the scope of coverage under any given cyber policy. That makes it important to consider what type of loss is included in the definition of "covered losses." For example, are PCI fees covered?[82] As discussed in more detail below, business accepting credit card payments frequently are contractually obligated to indemnify payment card service providers (intermediaries between the business and the credit card company) for fees levied against them by credit card companies for losses through cyber incidents. And even though those payments are ubiquitous in the industry, they can fall under exclusions for contractually assumed obligations. If the policyholder is a business that accepts credit card payments, it therefore needs to evaluate where it may be necessary to negotiate an endorsement excepting PCI Fee payments from that exclusion.

Similarly, an increasingly common type of cyber incident is "social engineering fraud," where employees of a business are induced, through fraudulent emails that typically appear to originate with co-workers, management, or vendors, to make payments to a fraudulent bank account maintained by the perpetrator of the fraud. Although some crime policies may cover such losses, crime policies typically only cover direct theft by employees or by someone without authority to initiate the transaction (that is, a hacker). But in the social engineering card context, the employees making the transfers are authorized to do so, and do not do so with the intent of stealing from their employer (and do not transfer the funds for their own benefit). On that basis, some courts have, as discussed above, held that crime policies do not provide coverage. And not all cyber policies do. Therefore, if a policyholder is concerned about social engineering fraud (for example, because it deals with lots of vendors or handles monetary transactions for third parties), seeking a policy that contains such coverage, or negotiating an endorsement that provides it, may be important.

[82] PCI Fees are fines assessed by credit card brands resulting from the failure to comply with the provisions of the Payment Card Industry Data Security Standard.

Another aspect of the "covered loss" issue is whether covered losses include data loss from physical breaches, such as the theft or loss of devices such as laptops, tablets, or smart phones. If, for example, a policyholder's employees travel frequently with such devices, it may be prudent to include such coverage.

The reason leading to a loss can be an important consideration in this context. For example, are losses resulting from cyber incidents that are directly or indirectly caused by employee negligence (such as the failure to use a secure password, or the failure to log out of the network overnight) covered? Does coverage extend to losses caused by unauthorized by employees (as opposed to third parties)? As always, there is no one-size-fits-all answer, but these issues need to be considered in the underwriting process.

Similarly, if a policyholder maintains a lot of data (whether its own or third parties') in the cloud, with a third-party storage or cloud vendor, it is important that coverage extend to losses of or damage to data managed by third parties and located on third-party systems. Moreover, there should be coverage for loss or business interruption caused by a cyber incident affecting the vendor's system. That can be accomplished in a variety of ways: by requiring the vendor to indemnify the policyholder, through the service agreement; by requiring the vendor to make the policyholder an additional insured under the vendor's cyber policy; or by ensuring that the policyholder's policy include such coverage. The important point is that, with cloud storage becoming ever more ubiquitous, this issue be addressed.

Finally, there is the potential issue of "BYOD" coverage. "BYOD" stands for "bring your own devices" and refers to situations in which a policyholder allows its employees to access the policyholder's systems through their own devices, such as smart phones and laptops. In that case, the policyholder may want to obtain BYOD coverage to protect itself against, e.g., malware or viruses transmitted to its systems from an employee device.

iii. Consultancy Services

Some, but not all, insurers providing cyber policies provide consultancy services to assist policyholders in assessing their data security practices, scan systems for threats, provide threat-mitigation services, and/or assist in responding to incidents. Depending on a given policyholder's sophistication in dealing with IT and cyber threats, these services can be very valuable.

iv. Sublimits

Like other policies, cyber policies can contain sublimits applicable to specific types of losses, such as losses resulting from cyber extortion or regulatory inquiries, or payments for crisis management and notification costs. As always, policyholders should be aware of these sublimits because they can significantly reduce available coverage for particular types of losses, and policyholders should negotiate endorsements raising sublimits if necessary.

v. Retroactive Date and Extended Reporting Period

Retroactive Date: Cyber policies typically provide coverage for cyber incidents that occurred after a specified date—that can be the date of policy inception or an earlier date called the "retroactive date." Regardless of what date is selected, there generally is no coverage for an incident that occurred before the specified date, but was discovered after the date. And since cyber incidents can take a significant amount of time to discover—months or even longer—this concept of a retroactive date becomes important in the cyber policy context, particularly for first-time purchasers of cyber coverage.

Of course, a longer period of retroactive coverage increases premiums, but that may well be worth it considering the cost of cyber breaches, which, in FY2017, where at $225.00 per breached record in the United States.[83] It may be advisable to obtain as much retroactive coverage as is financially feasible—insurers typically provide retroactive coverage periods of up to one year.

Extended Reporting Period: The extended reporting period is, in some ways, the mirror image of the retroactive date, at the termination side of the policy. In addition to requiring that the cyber incident occurred after the retroactive date, cyber policies typically also require that the policyholder's claim be reported to the insurer during the policy period—which obviously requires that the policyholder be aware of the incident. Here, again, the length of time that it can take to become aware of a cyber incident can be problematic: what happens if a breach occurs a few days prior to expiration of a policy period, but is not discovered for several months thereafter?

That is where the extended reporting period comes in, which gives policyholders extra time in which to notify insurers of a cyber breach (which still must have occurred in the period between the retroactive data and the policy termination date). At least 60 days after policy termination are typically recommended, though some insurers allow the purchase of up to 36 months of extended reporting.

vi. Exclusions

Cyber policies, like all other policies, contain exclusions that limit coverage. But, unlike the pollution exclusion or the intended-or-expected exclusion, some of the exclusions in cyber policies are not necessarily familiar to policyholders and may thus warrant particular attention.

Failure to Follow Minimum Required Practices: This provision excludes from coverage losses that result from the insured's failure to follow specified security and preventive practices. The required practices can be identified in an exhibit or endorsement to the policy, or make reference to practices identified by the insured in its application. Often, "shortcomings" in an insured's security practices may be identified during underwriting; if that is the case, those will need to be addressed in order to ensure that coverage will be available.

Failure to Follow Minimum Accepted Practices: This provision is similar to the one above, but more tricky, because "minimum accepted practices" typically refers to accepted industry standards and thus changes over time. As an example, a policyholder's encryption method may be a "minimum accepted practice" at the time of policy inception. But half-way through the policy period, the industry standard for encryption changes. The policyholder does not immediately

[83] Ponemon Institute, 2017 Cost of Data Breach Survey, at 5 (June 2017).

update its encryption protocol, and a breach occurs. In that situation, the insurer may well argue that there is no coverage because the policyholder did not comply with "minimum accepted practices."

Whether such arguments will be successful remains to be seen since, as discussed below, cyber-policy language is just now starting to be litigated. The point here is that policyholders need to both be aware of the potential pitfalls of this type of exclusion, and to keep abreast of industry developments. It is still unclear, though, how this type of exclusion will ultimately be treated because it requires a balancing of requiring adoption of best security practices and requiring adoption of new and untested technology too early, which can sometimes cause more problems than it fixes.

War and Terrorism: War and terrorism exclusions are becoming increasingly common in cyber policies. They exclude from coverage breaches perpetrated by foreign governments or by individuals that could be categorized as "foreign enemies" or "cyber terrorists." This type of exclusion would preclude coverage for, e.g., the Sony hack commonly believed to have been perpetrated by North Korea, and may also preclude coverage for incidents such as the WannaCry attack, which has also been traced back to North Korea. If attacks by such foreign governments, foreign enemies, or cyber terrorists are of concern to a policyholder, it could seek to obtain cyber terrorism coverage, which is starting to be available either as an independent policy or as a cyber-policy endorsement.

Personal Capacity Publication: Some policies contain exclusions for publications by employees in their "personal capacity," that is, on their personal blogs or social media sites, or in personal email. Under such an exclusion, no coverage would be available if an employee discusses third-party confidential information held by a policyholder in an email sent from his or her personal account. If that is a concern, policyholders may want to seek an endorsement (or consider alternative coverage).

Contractually Assumed Liability: This is a very common exclusion, in both cyber and other types of policies. But, as discussed below, it can have unintended consequences in the cyber context. If a policyholder is faced with such an exclusion, it should carefully review its vendor agreements to see whether there are any instances for which endorsements should be considered.

vii. Warranties and Incorporation of Application Materials

It is common practice for insurance policies to either incorporate application materials into the policy or contain warranties stating that all of the information in the application is accurate, correct, and complete, and was relied on by the insurer to issue the policy. In the cyber context, such provisions present some particular pitfalls resulting from the fact that many policyholders are not aware of, e.g., what data they are maintaining where, who has access to it, and how long the data is retained. Similarly, there is sometimes a disconnect between the Risk Management and IT or Data Security Departments, so that the risk managers completing applications with the brokers may have incomplete or outdated information. But errors in the application, even if unintentional, can result in denial of coverage under an incorporation provision, or rescission of the policy under a warranty. Failure to comply with procedures set forth in the application can have the same effect.

To avoid these pitfalls (to the greatest extent possible), policyholders should consider conducting a data audit and evaluating their security protocols before seeking cyber coverage. A data audit would provide detailed information about what data is retained where and by whom, who accesses the data, how long it is retained, and whether retention policies are complied with. It also would allow for adjustments to be made before an application is completed, and would provide as much knowledge as possible to ensure accuracy of the application. The same applies to an evaluation of security protocols: It provides a snapshot of the status quo, allows for the detection and remediation of deficiencies, and ensures that accurate information is provided to the insurer. It can be helpful to conduct these audits in consultation with outside coverage and data-security counsel.

viii. Limitations on Covered Locations

Another issue that can arise more frequently in the cyber context than with respect to some other policies is the limitation on covered locations. If a policyholder conducts business out-of-state, in neighboring countries, or globally, whether the policyholder actually has widespread locations or whether its employees travel widely, limitations on covered locations should be carefully reviewed. Failure to do so may, for example, preclude coverage if an employee's laptop is stolen on a layover in Singapore, when coverage is limited to the United States and its territories.

ix. Defense and Settlement

Third-party cyber policies raise the same issues as other types of policies in terms of defense and settlement: Who selects defense counsel? Who controls the defense? Do defense costs erode policy limits? Who gets to decide whether to settle? Is consent of the other party required? Does the policy contain a hammer clause? Of what type? As these questions are familiar and do not generally raise issues specific to cyber coverage, they are raised here only for completeness' sake, without a full discussion.

4. The Next Wave

a. Cases Involving Cyber Policy Provisions

As mentioned above, disputes about actual cyber policies (as opposed to cases seeking coverage for cyber-related losses under more traditional policies) are just now making their way into court (and even that subject to the policies' frequent arbitration provisions). There just are not many cases yet addressing cyber policies, much less decided cases. Nonetheless, this section provides an overview over relatively recent cases.

i. Cyber-Policy Coverage for Payment Card Industry (PCI) Fees

One of the early issues that has arisen in such litigation is whether cyber policies provide coverage for PCI fees assessed by credit card companies in case of a data breach for which the insured is ultimately liable. In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.*, the court answered that question in the negative under the cyber policy at issue there.[84]

[84] No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 26, 2016).

The relevant facts will sound familiar to anybody with experience with data breaches. As P.F. Chang's ("Chang's") allowed its customers to pay for their meals with credit cards, it had, as is standard practice in the industry, entered into a Master Service Agreement (the "Agreement") with Bank of America Merchant Services ("BAMS") under which BAMS processed credit card transactions for Chang's.[85]

The Agreement incorporated MasterCard's PCI rules, which provided, among other things, that MasterCard could assess fees against BAMS if MasterCard incurred losses from a data breach at a client of BAMS. The Agreement also contained an indemnification clause under which Chang's agreed to indemnify BAMS for any such fees assessed because of a breach at Chang's. All of that is standard and well known in the industry, including to insurers active in the industry.[86]

Chang's was eventually hacked, with the credit card numbers belonging to over 60,000 of Chang's customers being posted on the internet. As a result, MasterCard incurred costs for fraudulent charges on its customers' credit cards, for notifying customers of the hack, and for providing new credit cards and pins.

MasterCard then assessed about $1.72 million in fees against BAMS (the PCI Fees): $1.7 million was for fraudulent charges, and about $200,000 for the issuance of new credit cards and related costs. BAMS sought indemnification from Chang's, which Chang's provided because BAMS would otherwise have cut off its services to Chang's. Chang's then sought reimbursement for the PCI Fees under its cyber coverage with Federal Insurance Company (Federal). Federal denied the claim, and litigation ensued.[87]

The district court initially found that there was no coverage for the $1.7 million in fees for fraudulent charges because the policy required that the third party making the claim was the person whose confidential records had been disclosed ("injury sustained . . . by a Person because of . . . unauthorized access to **such Person's** Record" (emphasis added)).[88] But the disclosed records were not BAMS (the entity making the claim for indemnification); they belonged to MasterCard, and so there was no coverage.[89]

Then, although the court found at least potential coverage for the remaining approximately $200,000 in PCI Fees, it also concluded that those fees fell under an exclusion "for contractual obligations an insured assumes with a third-party outside of the Policy."[90] 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.[91] The court was not swayed by Chang's argument that it had to enter into the Agreement to allow its customers to pay by credit card.[92] Similarly, that Federal knew that indemnification of credit card processing services by their clients was standard practice was not relevant.[93] To the contrary, the court assumed that,

[85] *Id.*, at *2.
[86] *Id.*
[87] *Id.*
[88] *Id.*, at *4-5.
[89] *Id.*
[90] *Id.*, at *6, *7-8.
[91] *Id.*, at *8-9.
[92] *Id.*
[93] *Id.*, at *9.

since both Federal and Chang's were sophisticated parties, they had contracted for exactly the coverage they wanted, which clearly did not extend to any of the PCI Fees.[94] Chang's could have asked for such coverage, but did not.[95]

Chang's appealed, but the case settled while the appeal was pending, so that the district court's opinion is, at least for now, the last word on this issue. Consequently, if policyholders accept credit cards and contract with a credit card processing service, they should be aware of the following:

1. If their credit card processing agreement contains a clause obliging them to indemnify the service provider for PCI fees (which it probably does), they should review their cyber policy for a "contractually assumed liability" exclusion;

2. If there is such an exclusion, they should seek to negotiate an exception to it for PCI fees; and

3. They should beware of potential "**such** person" language in the definition of a "claim," and seek to have such language changed, or an endorsement added that specifically provides coverage for PCI fees, including fees for fraudulent credit card charges.

ii. Cyber-Policy Coverage for Costs Related to Data Breach and Publication of Patient Medical Records

The complaint filed in *Columbia Casualty Co. v. Cottage Health System* raised the issue of whether the relevant cyber policy provides coverage for costs related to a data breach at Cottage Health System's ("Cottage Health's") facilities that resulted in the publication of patient medical records.[96] Unfortunately, the California District Court did not get the opportunity to resolve this issue because the case was dismissed on January 25, 2018, based on the parties' stipulation for voluntary dismissal in favor of an apparently parallel state court proceeding. But as the issues raised in the complaint are important in the cyber-insurance context, they are nonetheless summarized below.

Cottage Health operates a network of hospitals in Southern California.[97] In late 2013, Cottage Health experienced a data breach that resulted in the public disclosure, on the internet, of over 32,000 electronic patient medical records.[98] The inevitable class action followed, which was eventually settled for $4.125 million.[99] Cottage Health notified Columbia of the suit, and Columbia defended, and funded the settlement, under a complete reservation of rights, incurring over $168,000 in defense costs, over $860,000 in data breach response costs, and the $4,125 million to fund the settlement.[100] Additionally, at some point before Columbia brought this suit, the California Department of Justice commended an investigation into potential violations of

[94] *Id.*
[95] *Id.*
[96] No. 2:16-cv-3759 (filed C. Dist. Cal.).
[97] *Cottage Health Sys.*, No. 2:16-cv-03759, Complaint at 1 (C. Dist. Cal. May 31, 2016). The following summarizes the allegations and claims in Columbia's complaint.
[98] *Id.* at 4.
[99] *Id.* at 2, 4.
[100] *Id.* at 2, 5.

HIPAA and various other federal and state statutes related to the data breach, exposing Cottage Health to potential liability for sanctions, fines, or penalties.[101]

The Columbia cyber policy at issue was a claims-made policy that was effective both when the breach occurred and when the class action (and presumably the California DOJ investigation) commended.[102] The policy provided coverage for data-breach related injuries or damages with a $10 million per occurrence and aggregate limit and a $100,000 SIR, and, separately, for up to $5 million in breach response and crisis management expenses.[103] The policy also contained an exclusion for "Failure to Follow Minimum Required Practices," that is, failure to follow both the procedures and risk controls identified in the application and ones contained in a Minimum Required Practices Endorsement.[104] Moreover, the policy contained conditions providing that (a) Cottage Health confirmed that all statements in its application were true, (b) the application materials were incorporated in the policy, and (c) Cottage Health's statements in the application were material to Columbia's acceptance of the covered risk.[105] Finally, the policy conditions provided that the policy would be null and void if the application contained misrepresentations or omissions that either were made with intent to deceive or materially affected acceptance of the risk by Columbia—which, according to the other condition mentioned above, was always the case.[106]

According to Columbia, Cottage Health's application included responses to a "Risk Control Self Assessment" that contained representations about Cottage Health's data security practices.[107] And Cottage Health warranted that all representations in the application were "true, accurate and complete, and that no material facts have been suppressed or misstated."[108] Columbia claimed that it justifiably relied on Cottage Health's representations in the application.[109] But, according to Columbia, its investigation of Cottage Health's claim revealed that the application actually contained misrepresentations because Cottage Health did not actually practice what it had described in the Self Assessment—for example, Cottage Health allegedly did not change software settings from factory defaults, did not regularly update security patches, had no threat management program, and did not track unauthorized access to its systems.[110]

Consequently, through its Complaint, Columbia sought the following relief: First, a declaratory judgment that, under the "Failure to Follow Minimum Required Practices" exclusion, Columbia had no obligation to defend Cottage Health in the underlying class action, or to indemnify it for costs related to the data breach.[111] Second, a declaratory judgment that Columbia had no obligation to defend Cottage Health in the pending California DOJ investigation because the policy's definition of "damages" did not include "criminal, civil, administrative or regulatory relief, fines or penalties."[112] Third, a declaratory judgment that the policy was void *ab initio* and

[101] *Id.* at 5.
[102] *Id.*
[103] *Id.* at 6.
[104] *Id.* at 7-9.
[105] *Id.* at 8-9.
[106] *Id.* at 9.
[107] *Id.* at 10-11.
[108] *Id.* at 11-12.
[109] *Id.* at 12.
[110] *Id.* at 13-14.
[111] *Id.* at 17-18.
[112] *Id.* at 19.

could be rescinded because Cottage Health's application, through the Self Assessment, contained material misrepresentations.[113] And fourth and finally, an order requiring Cottage Health to reimburse Columbia for the over $5 million in defense costs, data breach response expenses, and settlement funds it paid under its full reservation of rights, along with Columbia's costs and attorneys' fees.[114]

The complaint filed by Columbia highlights the above-mentioned importance for policyholders to carefully evaluate applications and accompanying materials to ensure their accuracy. Because of the potential dire consequences of misstating, even innocently, policyholders' data security practices or other required information, policyholders should consider involving their IT Professionals and CIO in the application process. And, once a cyber policy is issued, policyholders should, in coordination with their IT Professionals and, if necessary, outside coverage counsel, regularly review their cyber-risk management practices to ensure continued compliance with all applicable policy requirements. Finally, this complaint is a good example of how policy definitions—like the one of "damages" here that arguably precludes coverage for the California DOJ investigation—can serve to undermine what may be policyholders' expectations in obtaining the coverage.

b. Bad Faith

To date, there have been few reported decisions on bad faith claims against cyber insurers. While some breach of contract actions may also include bad faith claims, it is not clear whether breach of contract actions under cyber policies will follow that path.

Cyber policies and many of the terms they use are new. Moreover, if past is prologue, cyber villains will continue to find new ways to hack data and disrupt systems. These factors by themselves may provide arguments that an insurer's disclaimer cannot have been unreasonable or in gross disregard of the insured's interests, and thus cannot have been in bad faith, at least to the extent that policy terms have not been interpreted judicially and/or in the cyber context, or in the context of the particular threat at issue.

Some of the early cyber coverage cases discussed above have recognized this principle. In *Gulf Coast*, the court granted the insurer's motion for summary judgment on the issue of bad faith even though it found that there was coverage, explaining: "[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."[115]

Retail Ventures held that, while coverage existed, the insurer was not liable for bad faith for having disclaimed coverage.[116] First, a wrongful disclaimer is not, by itself, bad faith under Ohio law.[117] Additionally, the district court had concluded that the coverage question was fairly debatable, and the fact that the insurer did not reference the "resulting directly from" language in

[113] *Id.* at 20-22.
[114] *Id.* at 22-23.
[115] 2012 U.S. Dist. LEXIS 45184, at *13.
[116] 691 F.3d at 834-35.
[117] *See id*. at 834 (citation omitted).

its disclaimer letters and in the claim file did not demonstrate bad faith.[118] Moreover, the insurer's interpretation of Exclusion 9 (which, as discussed above, 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 esjudem generis did not apply."[119] 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."[120]

A district court in Utah recently rejected the fairly debatable doctrine, but not based on the coverage issues presented under the cyber policy at issue. In *Travelers Property Casualty Co. of America v. Federal Recovery Services*, the insured was in the business of handling, processing, storing, and transmitting electronic data for its customers.[121] One of its customers, a chain of fitness centers, alleged that the insured had improperly retained possession of gym members' account information, interfering with the insured's business dealings. The insured sought coverage under its cyber errors and omissions policy, and the insurer filed a declaratory relief action. The court ruled that the insurer had no duty to defend 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 insurer had acted knowingly, willfully, and maliciously; the court therefore granted summary judgment in the insurer's favor on the insured's counterclaim for breach of contract. As to the insured's counterclaim for bad faith, however, the court issued a mixed ruling. The court first ruled that, because the coverage provisions were not triggered, as discussed above, the insurer could not be liable for substantive bad faith. However, the court allowed the narrow issue of procedural bad faith to proceed to trial. Specifically, because the insured alleged that the insurer improperly required it to receive suit papers before initiating an insurance claim, and that the insurer did not "diligently investigate, fairly evaluate, and promptly and reasonably communicate with" the insured, factual disputes remained, and the fairly debatable doctrine did not allow summary judgment in favor of the insurer.[122]

Thus, so long as an insurer has conducted an appropriate investigation, it may be able to raise the genuine dispute or fairly debatable doctrines as affirmative defenses to bad faith allegations based on cyber claims

[118] *Id*. at 834-35.
[119] *Id.* at 835.
[120] *Id.*
[121] 156 F. Supp. 3d 1330 (D. Utah 2016).
[122] *Id.* at 1337-40.