MEALEY'S®
Emerging Insurance Disputes

2020 Cyber And Privacy Coverage – A Year In Review

by
Scott M. Seaman

Hinshaw & Culbertson LLP
Chicago, IL

and

Judith A. Selby

Hinshaw & Culbertson LLP
New York, NY

A commentary article reprinted from the January 7, 2021 issue of Mealey's Emerging Insurance Disputes

LexisNexis®

Commentary

2020 Cyber And Privacy Coverage – A Year In Review

By
Scott M. Seaman
and
Judith A. Selby

[Editor's Note: Scott M. Seaman is a Chicago-based partner with the national law firm of Hinshaw & Culbertson LLP and Co-Chair of the firm's global Insurance Services Practice Group. He focuses on complex first- and third-party insurance coverage and reinsurance law. Judith A. Selby is a New York-based partner of Hinshaw & Culbertson LLP. She focuses on complex first- and third-party insurance coverage litigation. The commentary is provided for general informational purposes only and is not intended to constitute legal advice. Any commentary or opinions do not reflect the opinions of Hinshaw & Culbertson LLP, their clients, or LexisNexis®, Mealey Publications™. Copyright © 2021 by Scott M. Seaman and Judith A. Selby. Responses are welcome.]

I. An Overview Of 2020 Cyber And Privacy Developments

Insurers have faced a wide range of cyber and privacy challenges in 2020 across various policy lines, some of which were exacerbated by the COVID-19 pandemic. In this article, we explore key issues and coverage developments impacting insurers in this evolving area.

To date, the vast majority of cyber coverage decisions have involved traditional first-party, third-party, and crime/fraud policies. Claims under those policies commonly are referred to as silent cyber or non-affirmative cyber claims. Most U.S. insurers have eliminated or substantially limited coverage for cyber losses under some of these policies. Where any coverage is afforded, it often is subject to relatively small sub-limits.

Prompted by a mandate from the UK Prudential Regulation Authority to either affirmatively cover or exclude cyber acts (malicious acts) and cyber incidents (accidental or operational error) by January 1, 2020, two UK insurance industry associations, the Lloyd's Market Association (LMA) and the International Underwriting Association of London (IUA), issued new cyber exclusions to eliminate or substantially limit potential coverage under those policies for cyber-related claims.[1] The "absolute" exclusion would preclude coverage for all cyber-related claims, and the less restrictive version contains a carve out for ensuing fire or explosion. The LMA also is considering revisions to the cyber war exclusion.[2]

Most insurers in the cyber insurance market now have issued several iterations of cyber-specific policies. Rulings under these policies are expected to be rendered with increasing frequency over the next couple of years.[3] Indeed, cyber insurers have experienced a steep increase in claims in 2020, driven primarily by ransomware claims, often coupled with data extraction, and business email compromise events. The costs associated with ransomware claims in particular have risen dramatically, due to increased ransom demands, threats to disclose extracted data, and related business interruption costs. To further raise the stakes associated with ransomware, the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN), both of which are creatures of the U.S. Department of the Treasury, issued advisories in October 2020 concerning ransom payments. The OFAC advisory stated: "Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response,

not only encourage future ransomware payment demands but also may risk violating OFAC regulation." The FinCEN advisory noted that "[e]ntities engaged in money services business activities (such as money transmission) are required to register as an MSB with FinCEN, and are subject to [Bank Secrecy Act] obligations, including filing suspicious activity reports (SARs)." The advisories underscore the complexity of responding to a ransomware event. They also highlight the importance of developing an appropriate incident response plan that addresses sanctions compliance and suspicious activity reporting obligations in the ransomware context.

In addition, the pandemic-driven, and largely unplanned, massive shift to remote work has created increased cyber risks that have already led to an uptick in cyber claims activity. The 2020 Allianz Cyber Risk Trends Report recently noted a small number of COVID-related cyber claims, while indicating that an increase in cybercrimes is likely.[4]

In the absence of comprehensive federal laws, individual states continue to adopt their own privacy laws and regulations. The groundbreaking California Consumer Privacy Act (CCPA) went into effect in January 2020. Similar to the EU's General Data Protection Regulation, the CCPA created a number of privacy rights for California consumers and obligations for businesses that collect and process personal information. Although the California Attorney General has yet to commence a CCPA enforcement action, several class action lawsuits have already been filed pursuant to the Act's limited private right of action. With the ink barely dry on the CCPA, California residents voted in November to approve the California Consumer Privacy Rights Act (CPRA), which further expands consumer privacy rights. The CPRA also creates a statewide privacy agency that will be charged with enforcement of privacy laws. This likely will lead to increased enforcement actions for privacy violations in California.

Class action cases, often culminating in multi-million dollar settlements, continue to be filed for alleged violations of the Illinois Biometric Information Privacy Act (BIPA). BIPA currently is the country's only biometric information privacy law with a private right of action.[5] Although BIPA settlements against social media giants like Facebook have garnered the most publicity, its important to note that BIPA claims have been filed against entities of all sizes. Many BIPA cases have arisen in the employment context, where biometric technologies are used for timekeeping and identity verification functions.

With all the focus this year on ransomware, BIPA, and CCPA, it is important to keep in mind that data breach class action litigation is continuing. The defense of those cases was further complicated in 2020 by successful challenges to the utilization of work product protection to shield forensic reports from discovery.[6]

In New York, a proposed amendment to the state's Civil Rights Law would create criminal liability for certain privacy violations, and the proposed It's Your Data Act would create CCPA-like consumer privacy rights, but with a broader private right of action. In July 2020, the New York Department of Financial Services, the state's powerful financial regulator, initiated its first enforcement action for alleged violations of its first-in-nation 2017 cybersecurity regulation.[7]

Several bills concerning the protection of biometric information are pending in the Massachusetts legislature, and comprehensive privacy bills were introduced in a number of states, including New Hampshire, Oregon, and Virginia. On the federal level, efforts in support of a comprehensive federal privacy law continue, and a biometric privacy bill was introduced in the U.S. Senate in August 2020.

In the European Union, a directive allowing representative collective actions for alleged violations of EU law in a broad range of areas, including data protection, was recently endorsed.[8] Uncertainty concerning international data flows remains following the Court of Justice of the European Union's July 2020 ruling to invalidate the EU-U.S. Privacy Shield in *Schrems II*.[9] The court also ruled that entities must assess, before transferring personal information, whether a third country provides adequate protection of that information. Although subsequent recommendations issued by the European Data Protection Board in November 2020 have provided some clarification, open issues concerning how to conduct that assessment increase in some respects the risks of unintentional noncompliance.

The continued proliferation of privacy and cyber laws will likely drive cyber insurance claims activity not only for data breach events, but also for information misuse

claims having nothing to do with a breach. These factors, combined with increasing data breach litigation costs and the rise of nation state cyber-attacks, may result in a further hardening of the cyber insurance market, as well as increased premiums, underwriting scrutiny, and coverage disputes.

II. 2020 Silent Cyber Coverage Cases

A. Ransomware

In January 2020, a federal district court in Maryland ruled that the first-party property coverage in a business-owner's insurance policy (BOP) covered the replacement of the insured's computer system after a 2016 ransomware attack. *National Ink and Stitch, LLC v. State Auto Property and Cas. Ins. Co.*, 435 F. Supp.3d 679 (D. Maryland 2020) (applying Maryland law). Following remediation, the system was still functional, but its performance was slowed by new protective software and it was likely that remnants of the virus remained on the system, increasing the risk of re-infection. The court determined that the 'loss of reliability, or impaired functionality demonstrate the required damage to a computer system, consistent with the 'physical loss or damage to' language in the policy." In our view, this decision does not materially advance efforts to secure cyber coverage under first party property policies for several reasons including that the 2016 National Ink policy at issue was written on the 1999 ISO form. More recent forms, such as the 2012 ISO BOP form, exclude computer-related losses.

B. Business Email Compromise

1. Management Liability Policy

A Mississippi federal district court ruled that Computer Fraud Transfer and Funds Transfer Fraud coverages were not applicable to losses resulting from an email phishing scam. *Miss. Silicon Holdings, LLC v. Axis Ins. Co.,* 440 F. Supp.3d 575 (N.D. Miss. 2020). The insured, Mississippi Silicon Holdings (MSH), had fallen prey to spoofed emails and wired more than $1 million to fraudsters instead of a legitimate vendor. Three MSH employees approved the wire transfers before MSH learned that hackers had infiltrated its computer system and impersonated an authentic vendor.

MSH's insurer accepted coverage under the Social Engineering provision of its management liability policy, but not under the Computer Fraud Transfer and Funds Transfer Fraud coverage grants, which contained substantially higher limits of liability. MSH instituted coverage litigation, alleging the loss fell within all three coverages.

The Computer Transfer Fraud provision covered losses resulting "directly from Computer Transfer Fraud that causes the transfer, payment, or delivery of Covered Property from the Premises or Transfer Account to a person, place, or account beyond the Insured Entity's control, without the Insured Entity's knowledge or consent." The Funds Transfer Fraud provision provided coverage for loss "resulting directly from the transfer of Money or Securities from a Transfer Account to a person, place, or account beyond the Insured Entity's control, by a Financial Institution that relied upon a written, electronic, telegraphic, cable, or teletype instruction that purported to be a Transfer Instruction but, in fact, was issued without the Insured Entity's knowledge or consent."

The court declined to adopted a proximate cause standard advocated by MSH, agreeing with the insurer that Computer Transfer Fraud coverage was not implicated because "nothing 'entered' into or 'altered' within [MSH's] Computer System . . . directly caused the transfer of any Money." Instead, the MSH employees caused the transfer. Because the fraudulent emails did not themselves manipulate MSH's computer system, a "Computer Transfer Fraud" did not directly cause the transfers. The court further held that the requirement for the transfer to take place "without the Insured Entity's knowledge or consent" was not satisfied. The court rejected MSH's assertion that a more logical reading of the requirement would be that MSH had to have actual knowledge of material facts, such as the transferee's true identity, stating that MSH provided no legitimate reason to impose a heightened requirement into the policy. The court distinguished the Social Engineering Fraud provision, which "clearly authorizes coverage when an employee relies on information that is later determined to be false or fraudulent. In contrast, the Computer Transfer Fraud provision specifically states that coverage is only available when the loss occurs 'without the insured entities knowledge or consent."

The court also held that the Funds Transfer Fraud coverage was not implicated because the MSH employees had knowledge of, and consented to, the transfers. The

court found no legitimate basis to accept MSH's argument that the policy required those MSH employees to know that the spoofed emails were fraudulent at the time of the transfers.

2. Crime Policy

In *Midlothian Enters. v. Owners Ins. Co.*, 439 F.Supp. 3d 737 (E.D. Va. 2020), a Virginia federal district court ruled a crime insurer had no obligation to cover losses resulting of an email phishing scam. In that case, a Midlothian employee had complied with an email request, purportedly from the company president, to wire more than $400,000 from Midlothian's bank account to a bank account in Alabama. Several days later, Midlothian discovered the email was fraudulent and tendered a claim to Owners Insurance Company, which denied coverage.

The crime policy provided coverage for theft of money and securities, but excluded coverage for "*[l]oss resulting from your, or anyone acting on your express or implied authority, being induced by a dishonest act to voluntarily part with title to or possession of any property.*" The court had no trouble deciding that the exclusion unambiguously precluded coverage. The court rejected the insured's attempt to create ambiguities in the exclusion by highlighting terms with more than one meaning or interpretations that conclude in different results in the interpretation of the exclusion." The court stated: "The fact that a word or phrase has more than one dictionary definition . . . does not make a provision ambiguous."

The court also rejected the insured's argument that a victim of fraud can never act voluntarily, and that the exclusion does not apply where the instruction to make payment is fraudulent: "The fact that another individual pretended to authorize the transaction does not negate the voluntariness of the transfer . . ." Consequently, "[a]llowing coverage of a fraudulently authorized transaction despite an exclusion based on '*any* dishonest act' would unreasonably limit the exclusion and render the provision meaningless." (Emphasis in original.)

3. Financial Institutions Bond

A New Jersey federal district court held that losses arising out of a phishing scam were not covered under a bank's Financial Institutions Bond. In *Crown Bank JJR Holding Co. v. Great Am. Ins. Co.*, 2020 U.S. Dist. LEXIS 23136 (D. N.J. Feb. 11, 2020) (New Jersey law), a fraudster impersonated Jackie Rodrigues, the wife of a senior executive of Crown Bank. In a series of 13 emails from a spoofed email address, the impersonator requested wire transfers from the Rodrigues's Crown Bank accounts to accounts in Singapore.

Pursuant to their customer agreement with Crown Bank, the Rodrigueses were permitted to request wire transfers by email, and Crown Bank was required to verify each request by calling the account holder at a designated phone number. Upon receipt of each of the fraudulent email requests, Crown Bank employees requested information needed to complete the transfer and emailed a wire transfer authorization form back to the impersonator. The impersonator would forge Mrs. Rodriguez's signature, and then email a PDF of the completed form back to the bank. Bank employees printed the PDF and then matched the forged signature on the form to the signature the bank had on file for Mrs. Rodrigues. Bank employees never called the designated phone number to verify the requests, even though the wire transfer form indicated that the call had been made. By the time the fraud was uncovered, over $2 million had been transferred from the Rodrigues's accounts. Crown Bank sought coverage for the loss under its Financial Institutions Bond and its Computer Crime Policy for Financial Institutions. Its insurer denied coverage under both policies, and coverage litigation ensued.

Crown Bank asserted that its claim was covered by Insuring Agreement D of the Financial Institutions Bond. That provision applied to:

> Loss resulting directly from the Insured having, in good faith, paid or transferred any Property in reliance on any **Written, Original** . . . (4) Withdrawal Order . . . (6) Instruction or advice purportedly signed by a customer of the Insured or by a banking institution . . . which (a) bears a handwritten signature of any maker, drawer or endorser which is Forgery; or (b) is altered, but only to the extent the Forgery or [alteration] causes the loss. **Actual physical possession of the items listed in (1) through (6) above by the Insured is a condition precedent to the Insured's having relied on the items.** [bolding added]

The term "Original" was defined as "the first rendering or archetype and does not include photocopies or electronic transmissions, even if received and printed." "Written" was defined as "expressed through letters or marks placed upon paper and visible to the eye."

The parties' central dispute was whether Crown Bank had actual physical possession of the "Written, Original" wire transfer forms, a condition precedent to coverage under Insuring Agreement D. The insurer argued that the Bank failed to satisfy that condition because printouts of the electronically transferred PDFs from the impersonator did not fall within the Bond's definition of "Original." Crown Bank contended that a PDF itself is not an electronic transmission, and each print out of a wire transfer authorization form from a PDF was a "first rendering" within the definition of "Original." The court rejected the Bank's arguments because "*documents transmitted electronically are not originals, even if received and printed*," according to the Bond. The Bank's additional contention that the "first rendering or archetype" language in the definition of Original was ambiguous as applied to PDFs also missed the mark: "Regardless of any ambiguity concerning whether a PDF may qualify as an 'Original' without electronic transmission, where a PDF (or any electronic file format) is transmitted electronically, it cannot qualify as an 'Original' as defined in the [Bond.]"

The court deferred ruling on whether there was coverage under the Computer Systems Fraud Insuring Agreement in the crime policy pending further briefing on the insured's objectively reasonable expectation of coverage under that policy.

4. Errors & Omissions Policy

In November, a New Jersey federal district court ruled that there was no coverage under a title agent's errors and omissions policy for losses resulting from an email phishing scam. In *Authentic Title Servs. v. Greenwich Ins. Co.*, No. 18-4131 (KSH) (CLW), 2020 U.S. Dist. LEXIS 215018 (D.N.J. Nov. 17, 2020, the title agent received emails purporting to be from a mortgage letter, directing the agent to transfer over $480,000 to a specified bank account and to confirm the transfer by email only. The emails were in fact sent to the agent by a fraudster. The agent followed the directions in the spoofed emails, but later realized that the funds had been transferred to a fraudulent account. By that time, the money had been withdrawn from the fraudster's account and could not be recovered. The agent then tendered a claim for the loss under its E&O policy. The insurer denied coverage, citing exclusion 14(a) for "the commingling, improper use, theft, stealing, conversion, embezzlement or misappropriation of funds or accounts."

In the subsequent coverage action, the court agreed with the insurer that the exclusion applied, stating: "[T]he terms undoubtedly apply to the . . . funds that [the agent] erroneously sent to the fraudster's account; it doesn't matter . . . who committed the theft or other prohibited act, the insured or another party; if the claim arose from such an act (and it cannot reasonably be disputed that it did), the plain and ordinary meaning of the language in exclusion 14(a) supports [the insurer's] denial of coverage."

The agent argued that exclusion 14(a) should not apply because the agent had no knowledge of the fraud. In support of that argument, the agent noted that policy exclusion 8 for "criminal, intentionally wrongful, fraudulent or malicious acts or omissions" exempts situations where the insured had no knowledge of the acts in question. The court stated:

> [The agent's] invitation to read exclusion 14(a) in the context of the policy as a whole helps [the insurer's] position rather than its own. [The agent] argues that exclusion 14(a) must be read to reach only conduct by the insured. But the language of other exclusions suggests that when [the insurer] intended that result, it expressly stated so. Exclusion 8 . . . includes the carve-out language . . . Exclusion 14(a) does not. As [the insurer] argues, this indicates that the company intended it to apply to conduct regardless of whether the insured was involved; in other words, this is the intended result of the language, rather than an unintended.

The court concluded that the policy "language is not ambiguous, and the Court rejects [the agent's] arguments to the contrary, including its resort to the doctrine of the insured's reasonable expectations and its reliance of decisions that found ambiguity in policy language bearing no resemblance to the . . . policy before the Court."

C. Privacy Violations

In *Brighton Collectibles, LLC v. Certain Underwriters at Lloyd's London*, 798 F. App'x 144 (9th Cir. 2020), an insurer was required to defend a putative class action alleging that the insured retailer collected and sold customers' personal information in violation of California's Song-Beverly Credit Card Act. The insured argued that the claim triggered its personal injury coverage, which applied to personal injury caused by an offense arising out of the insured's business, which includes "oral or written publication of material that violates a person's right of privacy." Based on California Supreme Court precedent holding that the overriding purpose of the Credit Card Act is to protect the personal privacy of consumers, the Ninth Circuit found that the class action alleged an invasion of privacy sufficient to trigger the insurer's duty to defend. The court rejected the insurer's assertion that coverage was barred by the policies' exclusions for "advertising, publishing, broadcasting or telecasting done by or for" the insured. The court stated: "The word 'publishing' in this coverage exclusion cannot be read to have the same meaning as the word 'publication' in the personal injury provision. Such a reading would exclude coverage for virtually any publication over which [the insured] might realistically be sued, rendering the policies' express coverage for publications that violate privacy rights practically meaningless." The court also noted that the "grouping of 'publishing' with 'advertising. . ., broadcasting or telecasting' in the coverage exclusion suggests that the exclusion applies only to broad, public-facing marketing activities."

In another case addressing the "publication" requirement for personal injury coverage, an Illinois state appellate court ruled that a customer's biometric privacy class action claims against an insured tanning salon potentially fell within two insurers' personal injury coverage. *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*, 2020 IL App (1st) 191834 (March 20, 2020). The plaintiff in the underlying class action alleged that the salon violated BIPA in connection with its collection of her fingerprint scan to enable her to access the salon.

Even though the plaintiff's biometric information was shared only with the vendor who implemented the salon access technology, the court ruled that the policies' "publication" requirement was satisfied. The court also held that an exclusion for "violation of statutes that govern emails, fax, phone calls, or other methods of sending materials or information" did not apply, even though the fingerprint scan had been sent to the vendor allegedly in violation of BIPA. The court ruled that the exclusion applies to laws that govern "*methods* of communications," not to laws like BIPA, which "limit the sending or sharing or certain information." This decision has been criticized, particularly on the ground that "publication" requires widespread distribution of the material at issue to the public under Illinois precedent.

III. Looking Ahead

On the coverage litigation front, even though insurers were largely successful in defending silent cyber claims in 2020, we expect that policyholders – particularly those who have not obtained cyber insurance – will continue to seek coverage for privacy and cyber claims under non-cyber policies. Insurers are urged to closely following legal and regulatory developments in this area and to consider their underwriting procedures and policy wordings across all coverage lines in light of these emerging and often high-stakes risks. Currently there is a relative dearth of judicial decisions interpreting and applying cyber-specific policies. However, we expect that, over the next couple of years, the pace of judicial decisions under cyber-specific policies will increase markedly.

Endnotes

1. For the language of the exclusions, *see* S.M. Seaman and J.A. Selby, "Insurers Take Steps to Reduce Silent Cyber Exposures," *Hinshaw Insights for Insurers* (Feb. 10, 2020), available at https://www.hinshawlaw.com/newsroom-updates-insurers-take-steps-reduce-silent-cyber-exposure.html.

2. *See* S&P Global Market Intelligence, Cyber Insurers Wrestle with War Exclusions as State-Sponsored Attack Fears Grow (Jan. 30, 2020), available at https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-wrestle-with-war-exclusions-as-state-sponsored-attack-fears-grow-56743302.

3. *See* S.M. Seaman and J.R. Schulze, *Allocation of Losses in Complex Insurance Coverage Claims* (Thomson Reuters 9th Ed. 2020-21) at Chapter 17 (Cybersecurity and Privacy Claims).

4. AGCS Trends in Cyber Risk 2020 (Nov. 2020), available at https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2020.html.

5. *See* S.M. Seaman, J.A. Selby and J.E. DeLascio, "Insurance Coverage for Biometric Claims," *New York Law Journal* (Oct. 2, 2020).

6. *See In Re: Capital One Consumer Data Security Breach Litigation,* MDL No. 1:19md2915 (AJT/JFA) (E.D. Va. May 26, 2020) (Mem Op.).

7. In the Matter of: First American Title Ins. Co., No. 2020-0030-C (N.Y.D.F.S), available at https://www.hinshawlaw.com/assets/htmldocuments/Blogs/Consumer%20Crossroads/first_american_notice_charges.pdf.

8. *See* E.U. Parliament Directive, available at https://data.consilium.europa.eu/doc/document/ST-9573-2020-REV-1/en/pdf.

9. *See Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems,* Case No. C-311/18, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9710189. ■

MEALEY'S: EMERGING INSURANCE DISPUTES
edited by Jennifer Hans
The Report is produced twice monthly by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 1087-139X