HINSHAW

Part Five: Reviewing Key U.S. Insurance Decisions, Trends, & Developments

Cyber Security And Privacy Insurance Claims

Insights for Insurers Alert | 10+ min read
Mar 3, 2022

This is the fifth installment of our series of articles reviewing some of the key trends and developments currently impacting the U.S. insurance industry.

To date, the vast majority of cyber coverage decisions have involved traditional first-party, third-party, and crime/fraud policies. Claims under these policies are commonly referred to as silent cyber claims. Most insurers in the cyber-insurance market have now 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.

- Indeed, cyber-insurers experienced a steep increase in claims over the past couple of years, driven primarily by ransomware, 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. The pandemic-driven massive shift to remote work spurred additional cyber claims activity. As a result, industry leaders are anticipating a hardening of the cyber-insurance market, as well as increased premiums and underwriting scrutiny.
- Zurich and Advisen's 11th Annual Information Security and Cyber Risk Management Survey was released in October 2021.[1] Among the interesting finding, 83% of respondents now buy cyber insurance, with 66% carrying stand-a-lone cyber policies.[2] The survey concluded that triple-digit premium increases, vanishing capacity, shrinking coverage, and shifted expectations around baseline controls have joined long-term frustrations over inconsistent policy language to create a truly challenging renewal process for insurance buyers. Uncertainties around risk assessment and incident response are major concerns.[3]
- According to the survey, ransomware has risen to the top of priority lists worldwide. For the first time, cyber extortion/ransomware has pulled even with data breach, with 95 percent of respondents selecting it as a coverage they expect to be included in their policies.[4] It was followed by data restoration at 90 percent, business interruption at 80 percent, and system failure coverage and bricking at 73 percent.[5] Results show that cyber

risk management has significantly increased in priority to companies—86 percent say it is a significant concern and they have taken steps to assess their risk; 65 percent have invested in cybersecurity solutions to mitigate risk; and 61 percent say risk managers and IT work together to monitor risk. The "unknowns" of ransomware may be the biggest issue for risk managers.[6]

Property Insurance

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.[7] 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.[8] 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."[9]

This decision does not materially advance efforts to secure cyber coverage under first-party property policies. While the *National Ink* policy was issued in 2016, it was primarily based on the 1999 ISO form. More recent forms, such as the 2012 ISO BOP form, exclude computer-related losses.

In Ohio, a policyholder sought coverage under the Electronic Equipment Endorsement in the property section of its business owner's policy for costs to restore data following a ransomware attack. The Endorsement defined "media" as "materials on which information is recorded such as film, magnetic tape, paper tape, disks, drums, and cards" and included electronic data stored on such media. The insurer contended there was no coverage because "[n]o film, magnetic tape, disc, drum, card, etc., have been identified as physically damaged in [the] claim." The court rejected that argument because the computer software and reproduction of data was contained on policyholder's servers, which also met the definition of media. At a minimum, there were disputed issues of fact as to whether the insured's computer system could have suffered "direct physical loss" and as to whether the insurer conducted an adequate coverage investigation.[10]

Business Email Compromise

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.[11] 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.[12] Three MSH employees approved the wire transfers before MSH learned that hackers had infiltrated its computer system and impersonated an authentic vendor.[13]

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 had much higher limits of liability.[14] MSH instituted coverage litigation, alleging the loss fell within all three coverages.[15]

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."[16]

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."[17]

The court declined to adopt 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."[18] Instead, the MSH employees caused the transfer, and thus, because the fraudulent emails did not themselves manipulate MSH's computer system, a "Computer Transfer Fraud" did not directly cause the transfers.[19]

The court further held that the requirement for the transfer to take place "without the Insured Entity's knowledge or consent" was not satisfied.[20] 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.[21] 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."[22] In contrast, the Computer Transfer Fraud provision specifically states that coverage is only available when the loss occurs "without the insured entity's knowledge or consent."[23]

The court also held that the Funds Transfer Fraud coverage was not triggered because the MSH employees had knowledge of, and consented to, the transfers.[24] The court found no legitimate basis to accept MSH's argument that the policy required those MSH employees to know the spoofed emails were fraudulent at the time of the transfers.[25] The decision was affirmed by the Fifth Circuit in 2021.[26]

In *Midlothian Enters. v. Owners Ins. Co*., a Virginia federal district court ruled a crime insurer had no obligation to cover losses resulting from an email phishing scam.[27] In that case, a Midlothian employee had complied with an email request from the company president and purportedly wired more than $400,000 from Midlothian's bank

account to a bank account in Alabama.[28] Several days later, Midlothian discovered the email was fraudulent and tendered a claim to Owners Insurance Company, which denied coverage.[29]

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."[30] 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."[31]

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 . . . ."[32] 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."[33]

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.[34] *In Crown Bank JJR Holding Co. v. Great Am. Ins. Co*., a fraudster impersonated Mrs. Jackie Rodrigues, the wife of a senior executive of Crown Bank.[35] In a series of 13 emails from a spoofed email address, the impersonator requested wire transfers from the Rodrigueses' Crown Bank accounts to accounts in Singapore.[36]

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.[37] 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.[38] The impersonator would forge Mrs. Rodrigues's signature and then email a PDF of the completed form back to the bank.[39] 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.[40] 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.[41] By the time the fraud was uncovered, over $2 million had been transferred from the Rodrigueses' accounts.[42] Crown Bank sought coverage for the loss under its Financial Institutions Bond and its Computer Crime Policy for Financial Institutions.[43] Its insurer denied coverage under both policies, and coverage litigation ensued.[44]

Crown Bank asserted that its claim was covered by Insuring Agreement D of the Financial Institutions Bond, which 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."[45]

The term "Original" was defined as "the first rendering or archetype and does not include photocopies or electronic transmissions, even if received and printed," while "Written" was defined as "expressed through letters or marks placed upon paper and visible to the eye."[46]

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."[47] Crown Bank contended a PDF itself is not an electronic transmission, and each printout of a wire transfer authorization form from a PDF was a "first rendering" within the definition of "Original."[48]

The court rejected the Bank's arguments because "documents transmitted electronically are not originals, even if received and printed," according to the Bond.[49] 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]."[50]

In Minnesota, a federal district court ruled that a retailer is not entitled to coverage under a commercial general liability policy for suits brought against it by credit card companies following a computer hack that exposed confidential financial data. [51] The court reasoned that the policyholder has not satisfied its burden to demonstrate that the data breach had not resulted in a "loss of use" of "tangible property that is not physically injured."[52]

In *G & G Oil Co. of Indiana v Continental Western Ins. Co*., the Indiana Supreme Court weighed in on cyber security in the context of a multi-peril policy's commercial crime and fidelity coverage. The court concluded the term "fraudulently cause a transfer" equates "to obtain by trick."[53] The court noted that every ransomware attack is not necessarily fraudulent. For example, if no safeguards were put in place, it is possible a hacker could enter a company's servers unhindered and hold them hostage. There would be no "trick." Thus, a question of fact exists precluding the entry of summary judgment in favor of the policyholder. The court found there is sufficient causal connection between the alleged fraud and the policyholder's use of the computer.[54] Its transfer of Bitcoin was nearly an immediate result of using a computer. Though the policyholder's transfer was voluntary, it was made only after consulting with the FBI and other computer tech services and was made under duress. Under those circumstances, the "voluntary" payment was not so remote that it broke the causal chain.[55]

The U.S. Court of Appeals for the Fifth Circuit recently affirmed the lower court ruling that policyholder RealPage could not recover under primary or excess commercial fraud policies.[56] The Fifth Circuit ruled that RealPage never "held" the funds intended for its property manager clients—a requirement to implicate coverage—when its employee clicked a fake link and gave information about the company's third-party payment processor.[57]

Privacy Violations

While Connecticut, Mississippi, Nevada, and Texas enacted revisions to their breach notification laws in 2021, two states passed privacy laws. Both the Virginia Consumer Data Protection Act and Colorado Privacy Act will take effect in 2023.[58]

In the absence of comprehensive federal laws, individual states continue to adopt their own privacy laws and regulations. For example, the ground-breaking California Consumer Privacy Act ("CCPA") went into effect in January 2020.[59] Similar to the European Union'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. Despite the recent enactment of the CCPA, California residents voted in November to approve the California Consumer Privacy Rights Act ("CPRA"), which further expands consumer privacy rights.[60] The CPRA also creates a state-wide privacy agency that will be charged with the enforcement of privacy laws. This likely will lead to increased enforcement actions for privacy violations in California.

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 with an even broader private right of action.[61] 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.[62]

In July, 2021, New York City's Biometric Identifier Law went into effect.[63] This law prohibits the sale or exchange for anything of value of biometric identifier information and requires commercial establishments that collect or store biometric identifier information to provide clear and conspicuous written notice at the establishment's entrance.[64]

Increased regulatory enforcement and the further proliferation of privacy and cyber laws and regulations will likely drive increased cyber-insurance claims activity for both breach and information misuse events going forward.

Several decisions on the privacy front were issued in 2020. In *Brighton Collectibles, LLC v. Certain Underwriters at Lloyd's London*, 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 "Credit Card Act").[65] 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."[66]

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.[67] 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."[68] 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."[69]

The Illinois Supreme Court found that a claimed violation of Illinois' Biometric Information Privacy Act ("BIPA") fell within (or potentially within) business owners' liability policies affording personal and advertising injury coverage.[70] In that case, the plaintiff in the underlying suit alleged she purchased a membership from the policyholder, a salon that granted her access to other salons.[71] Enrolling in the program purportedly required that the plaintiff have her fingerprint scanned in order to verify her identity.[72] The plaintiff alleged that the policyholder never provided her with, nor did she sign, a release allowing the policyholder to disclose her biometric data to any third party; nevertheless, the policyholder purportedly disclosed her fingerprint data to an out-of-state third-party vendor.[73] The plaintiff asserted claims for violation of BIPA, unjust enrichment, and negligence.

Because the policies did not define "publication," the court turned to the term's dictionary definition and applicable case law.[74] Ultimately, the court held that " 'publication' has at least two definitions and means both the communication of information to a single party and the communication of information to the public at large."[75] As such, the salon's disclosure of fingerprint data to another party constituted a "publication."[76] The court held the violation of statutes exclusion did not bar coverage for the claim since BIPA was dissimilar from the statutes enumerated in the exclusion.[77]

In *Massachusetts Bay Insurance Co. v. Impact Fulfillment Services*, the district court found that the general liability insurers had no duty to defend their policyholder, Impact Fulfillment Services ("Impact"), in a proposed class action from Impact's Illinois employees.[78] The underlying suit alleged that Impact scanned workers' fingerprints to track work hours without their consent, in violation of BIPA.[79] Contrary to the Illinois Supreme Court's decision in *West Bend*, the North Carolina federal court found the distribution of materials exclusion bars

coverage for the exact type of illegal information collection regulated by BIPA.[80] Applying North Carolina law, the court noted the exclusion in the policies before it—which was revised in 2013 by ISO—was broader than the exclusion in *West Bend*.[81] Specifically, the exclusion included the terms "printing, dissemination, disposal, collecting and recording" of information and materials.[82] The exclusion also bars coverage for violations of the Fair Credit Reporting Act, in addition to violations of the Telephone Consumer Protection Act and Can-Spam Act, which were also barred under the earlier version of the exclusion.[83] By contrast to the Illinois Supreme Court, the North Carolina federal court concluded that "BIPA is of the same kind, character and nature" as the Telephone Consumer Protection Act, the Fair Credit Reporting Act and other federal and state statutes for which coverage is barred by the exclusion.[84] An Illinois Appellate Court decision ruled that actions under section 15(c) and 15(d) of BIPA are governed by a one-year statute of limitations, but actions under section 15(a), 15(b), and 15(e) are governed by a five-year statute of limitations.[85]

Cyber security and privacy claims and litigation will continue to occupy insurers on both the claims and underwriting side for many years to come.

- Part One: Environmental, Social, and Governance (ESG)
- Part Two: Social Inflation
- Part Three: COVID-19 Business Interruption Coverage Litigation
- Part Four: Civil Unrest, Riots, And Strikes

---

[1] Zurich North American and Advisen Ltd., *11th Annual Information Security and Cyber Risk Management Survey,* (Oct. 26, 2021).

[2] *Id*.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Co*., 435 F. Supp. 3d 679, 680 (D. Md. 2020).

[8] *Id*. at 681.

[9] *Id*. at 686.

[10] *Emoi Servs., LLC v. Owners Ins. Co.* , 2021-Ohio-3942, ¶ 37 (Ct. App.).

[11] *Miss. Silicon Holdings, LLC v. Axis Ins. Co*., 440 F. Supp. 3d 575, 585 (N.D. Miss. 2020).

[12] *Id*. at 578.

[13] *Id*.

[14] *Id*. at 579.

[15] *Id*.

[16] *Id.*

[17] *Id*.

[18] *Id*. at 582.

[19] *Id.* at 582-84.

[20] *Id*.

[21] *Id*.

[22] *Id.*

[23] Id. at 585.

[24] *Id.*

[25] *Id.*

[26] *Miss. Silicon Holdings, LLC. v. Axis Ins. Co*., 843 F. App'x 581, 582 (5th Cir. 2021).

[27] *Midlothian Enters. v. Owners Ins. Co*., 439 F. Supp. 3d 737, 741 (E.D. Va. 2020).

[28] *Id.* at 740.

[29] *Id*.

[30] *Id*.

[31] *Id*. at 742.

[32] *Id*. at 743.

[33] *Id*. at 742 (emphasis in original).

[34] *Crown Bank JJR Holding Co. v. Great American Insurance Co.*, No. 16-8778, 2020 U.S. Dist. LEXIS 23136, at *1 (D.N.J. Feb. 11, 2020)

[35] *Id*. at *2.

[36] *Id.* at *3-4.

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.* at *5.

[43] *Id.*

[44] *Id.*

[45] *Id.* at *9-10.

[46] *Id.* at *10.

[47] *Id.*

[48] *Id.* at *11.

[49] *Id.* at *11-12.

[50] *Id.* at *12.

[51] *Target Company v. ACE American Ins. Co.,* 517 F. Supp. 3d 798, 806 (D. Minn. Feb. 8, 2021).

[52] *Id*. at 802-03.

[53] *G & G Oil Co. of Ind. v. Cont'l W. Ins. Co.* , 165 N.E.3d 82, 89 (Ind. 2021).

[54] *Id.* at 90.

[55] *Id.*

[56] *RealPage, Inc. v. Nat'l Union Fire Ins. Co.*, No. 21-10299, 2021 U.S. App. LEXIS 37962, at *14 (5th Cir. Dec. 22, 2021).

[57] *Id*.

[58] *See* Va. Code Ann. § 59.1-575 (effective January 1, 2023); Colo. Rev. Stat. § 6-1-1301 (effective July 1, 2023).

[59] Cal. Civ. Code § 1798.198 (2020).

[60] *The CCPA Wheels Keep Turning: The Addition of CPRA*, The Nat. Law Rev., (Nov. 5, 2020).

[61] *See* S. S9073, 2019 Leg. Sess. (N.Y. 2020).

[62] S. S5575B, 2019 Leg. Sess. (N.Y. 2019).

[63] N.Y.C. Admin. Code § 22-1201 (2021).

[64] *Id*.

[65] *Brighton Collectibles, Ltd. Liability Co. v. Certain Underwriters at Llyod's London*, 798 F. App'x 144, 145 (9th Cir. 2020).

[66] *Id.*

[67] *Id.*

[68] *Id.* at 146.

[69] *Id.*

[70] *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc*., 2021 IL 125978, *1.

[71] *Id.* at *4.

[72] *Id.*

[73] *Id.*

[74] *Id.* at *38.

[75] *Id.* at *43.

[76] *Id.* at *62.

[77] *Id*.

[78] *Massachusetts Bay Insurance Co. v. Impact Fulfillment Services, LLC,* No. 1:20CV926, 2021 U.S. Dist. LEXIS 182970, at *1 (M.D.N.C. Sep. 24, 2021).

[79] *Id.* at *6.

[80] *Id.* at *18.

[81] *Id.* at *17.

[82] *Id*.

[83] *Id.* at *17-18.

[84] *Id*. at *18.

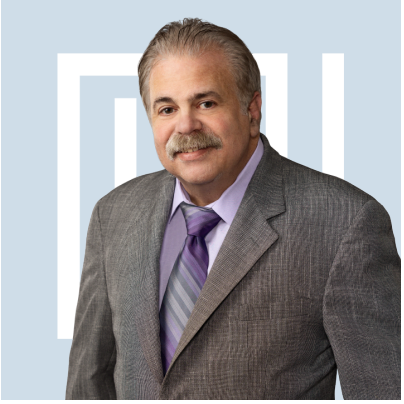
[85] *Tims v. Black Horse Carriers, Inc.*, No. 1-20-0563, 2021 IL App (1st) 200563 (Ill. App. Ct. 1st Dist. Sept. 17, 2021).

Related People

Sarah Anderson

Associate

312-704-3091



Scott M. Seaman

Partner

312-704-3699

Related Capabilities

Insurance

Insurance Coverage Litigation & Counseling