Parsing the Potential Challenges of Cyber Insurance Coverage

By Andy Rowlett

Threats to the security of attorney and law firm data in computers, networks and cloud services appear to be at an all-time high, according to the American Bar Association (ABA). ABA Formal Opinion 483 states that "the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be."[1] According to *Security* magazine, the first quarter of 2022 was marked by repeated ransomware strikes, geopolitical conflict and governmental action to protect users from cybersecurity threats.[2]

A review of the need for cyber insurance coverage should be a part of the risk assessment process for law firms of all sizes, per the ABA's 2021 cybersecurity report.[3] Insurance coverage for cyber losses has become a critical part of preparing for and responding to these threats. This article discusses several recent court opinions from cyber coverage lawsuits to increase readers' understanding of how to protect against cyber injuries, including identifying potential scenarios that might not be covered by your policy.

This article was reprinted by Howell & Fisher, PLLC, with permission from the Tennessee Bar Association.

Phishing Losses May Not Be Covered

Losses caused by a fraudulent funds transfer due to phishing may not be covered because of territorial limitations. Phishing is a social engineering tool used to fool someone into transferring funds to a fraudster. It often comes in the form of an email or website solicitation from a source that appears legitimate.

A Quality Plus employee received several emails apparently from the president of Quality Plus instructing her to wire hundreds of thousands of dollars to banks in Mexico and Hong Kong in payment of multiple invoices.[4] Another member of Quality Plus's accounting team approved four of the five transfers, which were completed. By the time the errors were discovered and investigated, the receiving back accounts had zero balances, and the funds could not be recovered.

Quality Plus had cyber insurance with National Union. The policy included a Funds Transfer Fraud Provision stating: "The Insurer will pay for loss of Funds resulting directly from a Fraudulent Instruction directing a financial institution to transfer, pay or deliver Funds from the Insured's Transfer Account." The "Fraudulent Instruction" definition included: "an electronic, computer, telegraphic, cable, teletype, telefacsimile, telephone or written instruction initially received by the Insured which purports to have been transmitted by an Employee but which was, in fact, fraudulently transmitted by someone else without the Insured's or the Employee's knowledge or consent."

National Union denied Quality Plus's request for coverage. One ground was the Policy's Territory Condition, which states, "This Crime Coverage Section covers loss that the Insured sustains resulting directly from an Occurrence taking place within the United States of America (including its territories and possessions), Puerto Rico and Canada." Because the parties disputed the location from which the sender transmitted the emails, the court could not determine whether coverage applied under the Policy's Territory condition and sent the matter to the jury.

Know Your Internal Policies

Failure to comply with an insured's own internal policy may prevent coverage for the insured. Internal policies of an insured may be determined by looking to what an insured states in its application for insurance. Also, a misrepresentation by a fraudster may not be covered if the fraudster is not pretending to work for an entity that has a direct relationship with the insured, such as a vendor.

ANDY ROWLETT has been practicing law with Howell & Fisher PLLC for over 28 years. He is also a mediator and arbitrator. Rowlett primarily handles personal injury claims, property losses (subrogation and recovery), insurance coverage matters and commercial disputes.

An unidentified threat actor impersonated a mortgage lender and fraudulently induced Star Title to wire funds to an incorrect account during the closing on a home sale.[5] After the loss, Star Title tendered its claim to Illinois Union, which had sold it a Cyber Protection Package Policy. Illinois Union denied the tender.

While the policy included a cybercrime endorsement with a Deceptive Transfer Fraud insuring clause, the endorsement required that the authenticity of each transfer request be verified in accordance with Star Title's internal procedures. The coverage was also limited to misrepresentations by a person purporting to be an employee, customer, client or vendor.

While the record was not clear about Star Title's internal procedures, Star Title had indicated in its application for coverage that it verbally authenticated wire instructions. Star Title did nothing to verify the authenticity of the transfer request. Its practice of having one employee file the incoming instructions while a second employee compared the final direction to the bank to the unverified instructions did not qualify as verifying authenticity.

Additionally, the mortgage lender was not Star Title's employee, customer, client or vendor. The lender did not sell a product or a service to Star Title; it only originated and serviced loans. The court declined Star Title's argument that the policy included any persons and entities involved in the real estate transaction.

CGL Coverage

Theft of credit card data by hackers may constitute a violation of a person's right of privacy, which triggers Commercial General Liability (CGL) coverage even if the subject claim is not made by the credit card customers or under a cyber policy. Cyber insurance is designed to provide coverage for data breach events, privacy violations, and cyber-attacks. However, coverage may also be available under a CGL policy.

Landry's is a Texas company that operates retail properties.[6] It had a data breach involving an unauthorized installation of a program on its payment-processing devices. The unauthorized program obtained personal information from millions of customer credit cards, at least some of which was used to make unauthorized charges.

Landry's was sued in contract by its payment processor. The insurance carrier for Landry's, ICSOP, denied the request of Landry's for a defense. The district court ruled in favor of ICSOP on its denial, holding that the processor sued Landry's for breach of contract, not for cardholders' privacy claims.

On appeal, Landry's had to persuade the U.S. Fifth Circuit that the processor's complaint sought damages "arising out of" publication of material that violates a person's right of privacy. The court interpreted "publication" broadly because the policy referred to "oral or written publication, in any manner… ." Publishing includes merely exposing or presenting information to view. The court concluded that customer data was exposed to view when it

CONTINUED ON PAGE 26 >

was routed through affected systems and when hackers used it to make fraudulent purchases.

The Fifth Circuit then assessed whether the injury arose out of privacy violations. Because a person has a right of privacy in their credit card data which hackers stole and used, there were privacy violations. The court rejected ISCOP's argument that the processor's suit did not arise in tort, a requirement not included in the CGL policy. The Fifth Circuit reversed the summary judgment in favor of ICSOP entered by the district court and remanded the case for further proceedings.

Purchase Cyber Insurance Appropriate to Your Operations

In another wire transfer induced by fraud, a food distributor purchased commercial crime coverage.[7] It decided not to purchase Funds Transfer Fraud coverage. A hacker gained access to the email account of the distributor's vice president of operations. The hacker tricked the bank into wiring money from the distributor's account to other banks and companies in fifteen different transactions totaling approximately $1,462,000. The distributor demanded reimbursement from its insurance carrier based on its Forgery or Alteration coverage.

The court sided with the insurance company. Because the hacker used wire transfer authorization forms that were not covered by the language of the commercial crime coverage ("similar written promises, orders or directions"), the losses were not covered under that policy.

The court also considered the fact that the losses would have been covered by the Funds Transfer Fraud coverage which the distributor decided not to purchase and the fact that policy's crime coverage and its (unpurchased) Funds Transfer Fraud coverage were written to be exclusive and not to overlap.

In another matter involving a title agency employee falling victim to a scam, the insurance carrier's denial of coverage was upheld.[8] The insured had not purchased a computer crime policy or a fraudulent transfer policy. Instead, it purchased a professional liability policy, which covered errors or omissions in providing professional services. The ABL court found that the "Conversion Exclusion" in ABL's E&O policy barred coverage for the damages caused by the fraudster's conversion of funds. ("This insurance does not apply to nor shall we have the duty to defend or indemnify any 'claim' or 'suit' arising out of or from: ... 3. Any damages arising out of the commingling, conversion, misappropriation or defalcation of funds or other property.")

Is the Policy's Language Too Broad?

As with many other coverage disputes, the outcome of a cyber coverage dispute can vary based on small changes to the facts and/or policy language. The insured (Ryeco) discussed in the above section lost its bid for coverage. However, a May 2022 court opinion from Texas citing *Ryeco* found in favor of the insured.[9] The court agreed with the insurance carrier in citing *Ryeco* that more courts have concluded that forged emails or other false wire transfer authorizations are not negotiable instruments and therefore are excluded from forgery coverage. However, neither the insurance company nor its insured cited binding authority that required the *Reliance* court to side with either party. The court therefore reviewed the policy language and facts in depth. Because the policy's forgery coverage included "similar written promises, orders or directions to pay a sum certain in 'money,'" and because the provision did not include the word "negotiable," the *Reliance* court concluded that the policy's language was broad enough to cover the fraudulent emails and wire transfer instructions before it.

Defining 'Business Interruption'

Losses caused by a "man in the middle" cyber-attack may not qualify as covered Business Interruption losses. Fishbowl Solutions is a software company.[10] A fraudster obtained access to the email account of one of Fishbowl's accountants and then intercepted emails between Fishbowl's customers and the accountant. The fraudster directed customers of Fishbowl to pay outstanding invoices to the fraudster's account, which is called a "man in the middle" attack. Fishbowl demanded reimbursement of its losses under its Cyber Business Interruption coverage. Fishbowl claimed that its business operations were impaired by the fraud because its ability to receive payment and communicate with its customers was damaged. The carrier denied coverage, arguing that no actual

interruption of Fishbowl's services occurred that resulted in a loss of "business income" as defined by the policy.

Because this opinion resolved a motion to amend and not the merits of the dispute, the court did not issue a conclusive opinion. It did note, however, that the applicability of Business Interruption coverage to the circumstances of this case is an unresolved legal issue.

Conclusion

Cyber insurance is a key element in preparing for and responding to cyber incidents and losses. Categorizing a loss involving IT issues as a "cyber" loss does not mean it is automatically covered by insurance. As with other types of insurance, whether a loss is covered is controlled by the policy language, the specific facts of the matter and the applicable law. Hopefully, the considerations discussed in this article will help readers identify and manage cyber insurance challenges. |||

NOTES

1. American Bar Association, Standing Committee on Ethics and Professional Responsibility, "Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack," Oct. 17, 2018, www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf.

2. Lauver, Madeline, "Top 5 Cyber Threats of Q1 2022," *Security* magazine, May 19, 2022, www.securitymagazine.com/articles/97657-top-5-cyber-threats-of-q1-2022.

3. Ries, David G., American Bar Association's "2021 TechReport, Cybersecurity; Section 5: Cyber Insurance," www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/, accessed July 19, 2022.

4. *Quality Plus Servs., Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA.*, No. 3:18CV454, 2020 WL 239598, at *3 (E.D. Va. Jan. 15, 2020).

5. *Star Title Partners of Palm Harbor LLC v. Illinois Union Ins. Co.*, No. 8:20-CV-2155-JSM-AAS, 2021 WL 4509211, at *1 (M.D. Fla. Sept. 1, 2021).

6. *Landry's Inc. v. Ins. Co. of the State of Pennsylvania*, 4 F.4th 366 (5th Cir. 2021).

7. *Ryeco LLC v. Selective Ins. Co.*, 539 F. Supp. 3d 399, 401 (E.D. Pa. 2021).

8. *ABL Title Ins. Agency LLC v. Maxum Undem. Co.*, No. CV 15-7534 (CCC), 2022 WL 986271, at *7 (D.N.J. Mar. 31, 2022).

9. *Cent. Mut. Ins. Co. v. Reliance Prop. Mgmt. Inc.*, No. 05-21-00071-CV, 2022 WL 1657031, at *7 (Tex. App. May 25, 2022). See also *Valero Title Inc. v. RLI Ins. Co.*, No. 4:19-CV-443, 2021 WL 5154790, at *2 (S.D. Tex. Mar. 29, 2021) (holding that insurance policies are to be construed "one policy at a time" and assessing inapplicability of different policy language used for different types of coverage); *City of Unalaska v. Nat'l Union Fire Ins. Co.*, No. 3:21-CV-00096-SLG, 2022 WL 826501, at *8 (D. Alaska Mar. 18, 2022) (discussing many Computer Fraud Insuring Agreement ["CFIA"] appellate rulings which vary based on policy language, facts and state approaches to interpreting insurance policies).

10. *Fishbowl Sols. Inc. v. Hanover Ins. Co.*, No. 21CV00794SRNBRT, 2022 WL 1462697, at *5 (D. Minn. May 9, 2022).