LAW360®

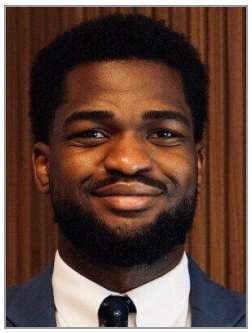
Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 New Cyberinsurance Rulings Aid In Policy Interpretation

By **Peter Halprin, Rebecca Schwarz and Simon Falokun** (October 16, 2025, 4:27 PM EDT)

Peter Halprin

Rebecca Schwarz



Simon Falokun

The global cyberinsurance market is expected to reach $30 billion by 2027. At present, 56% of the premium associated with cyberinsurance originates in North America.[1]

Although this market has exploded, there is no standardized cyber language or form shared by insurers and, at the same time, there are only a handful of decisions from around the country that have interpreted cyberinsurance policy language. Given this, policyholders, insurers and brokers are left with little guidance when disputes arise.

At the same time, because there is so little case law, the decisions that have been issued to date are of great importance and shed light on questions regarding the scope of coverage, causation and how to measure the period of restoration. Taken together, these cases provide policyholders, insurers and brokers with a sense of the evolving landscape and the direction in which the law appears to be developing.

In the last year, three new decisions have been issued that shed further light on the scope of coverage and causation issues, and further reinforce the direction in which the law appears to be developing.

Specifically, we discuss the following decisions below: (1) Abraham Linc Corp. v. Spinnaker Insurance Co., decided by the U.S. District Court for the Northern District of West Virginia; (2) Kane ex rel. N.M. Health Connections Inc. v. Syndicate 2623-623 Lloyd's of London, decided by the Court of Appeals of New Mexico; and (3) Connelly Law Offices PLLC v. Cowbell Cyber Inc. and Spinnaker Insurance Co., **decided** by the U.S. District Court for the Western District of Washington.[2]

Indeed, this interaction between the new decisions and the existing decisions reveals discernible trends in cyberinsurance jurisprudence that will continue to shape the underwriting of future policies and the handling of cyber claims.

Abraham Linc and the Scope of Computer and Funds Transfer Coverage

In Abraham Linc v. Spinnaker Insurance, decided on May 30, the Northern District of West Virginia was asked to interpret the scope of a computer and funds transfer fraud endorsement that was part of a cyberinsurance policy. Specifically, the court was asked to interpret whether coverage applied when the insuring agreement required "loss resulting directly from a fraudulent entry ... by a person or organization without authorization to access such computer system."

The dispute in Abraham Linc, or ALC, arose out of the hacking of a long-standing vendor of the company, which resulted in ALC's email systems being compromised. Ultimately, ALC sent a "substantial sum of money" via automated clearing house transfer to the vendor, consistent with the emailed directions from the vendor.

ALC was unable to recoup the money and put its broker on notice of its loss under its cyber policy. The insurer, Spinnaker, denied coverage on the grounds that ALC did not utilize a viable verification mechanism.

The court granted Spinnaker's motion to dismiss, concluding that ALC failed to plead facts that showed the loss resulted directly from unauthorized access to ALC's computer systems. The court looked to case law from other jurisdictions, primarily under crime insurance policies, wherein courts found that the rider language "applies to losses resulting directly from fraudulent access, not to losses from the content submitted by authorized users."

Additionally, the court reasoned that "[r]eading a [computer and funds transfer fraud] endorsement to cover all transfers that involved a computer and fraud would turn it into a general fraud policy."

The policy also contained a separate social engineering endorsement under which the court refused to dismiss ALC's claim. Although Spinnaker argued that there was no coverage because ALC did not comply with a condition precedent, whereby ALC had to follow a verification procedure before transferring the money to third-party accounts, ALC was able to show the court that it followed verification procedures such that dismissal was unwarranted.

While many cyber policies contain first- and third-party coverage, some also contain funds transfer and social engineering risks. To the extent cyber policies contain such coverage, Abraham Linc highlights the fact that given the dearth of cyberinsurance case law, courts may continue to look to the well-developed body of law regarding concepts like causation for funds transfer coverages under other policies such as crime insurance.

Notably, in this area, courts will closely scrutinize the triggering language, and the outcome of such analysis may differ significantly from state to state. For example, a New York court may have reached a contrary holding.[3]

It also bears noting, however, that a number of the early cyber rulings **discussed** in a previous Law360 guest column — such as Southwest Airlines v. Liberty Insurance Underwriters Inc., **decided** by the U.S. Court of Appeals for the Fifth Circuit last year, and New England Systems Inc. v. Citizens Insurance Co. of America, **decided** in the U.S. District Court for the District of Connecticut in 2022 — did address causation and so courts may, in the future, look to these rulings for guidance.

Kane and Connelly: Coverage for Third-Party Liability Claims

Picking up on the interplay between first- and third-party coverages in cyber policies, Kane v. Lloyd's of London, decided on June 16, demonstrates how the unique structure of cyberinsurance can lead to losses arising under both.

In a typical fact pattern, a company could be the victim of a ransomware attack, which would trigger various first-party cyber coverage, such as the payment of a ransom and breach response services. In the course of investigating the impact of the attack, it could come to light that the threat actors gained access to sensitive private data, which could, in turn, trigger notice to the affected parties and then result in a class action against the company, which would trigger third-party coverage.

The Kane decision involves a dispute regarding third-party coverage arising out of a fraudulent vendor invoice scheme. In April 2020, a third party posing as a senior accountant manager of one of the insured's vendors emailed a fraudulent invoice to New Mexico Health Connections and requested payment to the third party's bank account. In total, NMHC wired nearly $4.5 million in payments over the course of five transfers to the third party.

Since the money was sent to the wrong party, the vendor was never paid. The vendor sent a letter to NMHC demanding payment. NMHC reported the claim to Beazley, but Beazley denied coverage, claiming that the vendor's claim did not trigger third-party liability coverage under the policy.

The issue before the trial court, and on appeal, was whether the phrase "for ... a security breach" was broad enough to cover third-party liability arising from a security breach and not just the

security breach itself.

The Court of Appeals of New Mexico, focusing on the meaning of the preposition "for" and insurance policy rules of construction, affirmed the trial court ruling, held that the phrase was ambiguous and accepted NMHC's argument that it could be interpreted to provide coverage for a third-party claim arising out of a security breach causally connected to a loss.

Important in the court's analysis was the fact that the policy lacked a provision limiting third-party liability coverage for a security breach solely for the loss of data.

Similar to Kane, the issue in Connelly Law Offices v. Cowbell Cyber and Spinnaker Insurance, which **settled** on Oct. 6, also revolved around whether the phrase "for a Wrongful Act" was broad enough to cover a third party's criminal conduct.

In that case, hackers impersonated a law firm entitled to a payment and convinced Connelly, the insured law firm, to wire a payment of $1.5 million to a fraudulent account. As in Kane, since the money was sent to the wrong party, the party entitled to the funds was never paid. When fraud was eventually discovered, the party entitled to the funds brought a claim against the insured law firm.

As a result of the fraud and the resulting lawsuit, Connelly sought coverage under its commercial cyberinsurance policy. However, Cowbell Cyber and Spinnaker Insurance denied any indemnity obligation and denied coverage under the security breach liability insuring provision, arguing that the "Claim must be for a Wrongful Act" and that there was no strict causal connection between the claim and the wrongful act.

Like the Court of Appeals of New Mexico in Kane, the Western District of Washington focused on the meaning of the preposition "for" and insurance policy rules of construction in holding that the phrase was ambiguous and that the security breach liability insuring provision provided coverage.

The courts' readings in Kane and Connelly are consistent with the Southwest Airlines and New England rulings, as well as the U.S. District Court for the District of Minnesota's 2022 decision Fishbowl Solutions Inc. v. Hanover Insurance Co., wherein courts looked to the coverage grants and found that losses arising out of cyberincidents were causally covered under cyber policies.

What to Watch

The cases above demonstrate that businesses continue to face cyber threats and, given the potential financial implications, highlight the importance of cyberinsurance as a key component of a risk management strategy to address such hazards.

Although there is not a lot of case law out there interpreting cyberinsurance forms, the cases to date demonstrate that cyber coverage grants, which may include triggering terms such as "as a result of," "directly resulting from" or "for," will be read broadly by courts to include any losses that would not have occurred but for the cyberincident.

Peter A. Halprin is a partner, Rebecca Schwarz is an associate and Simon Falokun was a summer associate at Haynes and Boone LLP.

[1] https://actuary.org/wp-content/uploads/2025/08/Toolkit-GlobalCyber-8-25.pdf.

[2] Abraham Linc Corp. v. Spinnaker Ins. Co ., No. 1:23-CV-98, 2024 U.S. Dist. LEXIS 125363 (N.D.W. Va. July 16, 2024). Kane v. Syndicate 2623-623 Lloyd's of London , No. A-1-CA-41254, 2025 N.M. App. LEXIS 38 (Ct. App. June 16, 2025). Connelly L. Offices, PLLC v. Cowbell Cyber, Inc ., No. 25-cv-00302-JHC, 2025 U.S. Dist. LEXIS 152604 (W.D. Wash. Aug. 7, 2025).

[3] See Medidata Solutions Inc. v. Federal Ins. Co., 729 Fed. Appx. 117 (2d Cir. 2018).