Lowenstein Sandler

Client Alert

Insurance Recovery

July 16, 2018

Maximizing Insurance Coverage for Cyber Losses: Two New Decisions Highlight Potential Recovery

By Andrew M. Reidy, Joseph M. Saka, and Courtney E. Alvarez

What You Need To Know:

- **The U.S. Court of Appeals for the Second Circuit found coverage for a "spooking" attack under a crime insurance policy, and the U.S. Court of Appeals for the Fifth Circuit found their insurer had a duty to defend under a management liability insurance policy for claims alleging cyber-related losses.**
- **These cases highlight that cyber-related losses may be covered under traditional commercial insurance policies.**
- **Businesses should consider their insurance policies broadly in assessing whether there may be a recovery source for cyber-related losses.**

Businesses prudently and increasingly purchase stand-alone cyber insurance policies to manage the risk of cyber breaches and attacks. Two decisions from separate U.S. Courts of Appeals in the past two weeks highlight the fact that in-house counsel and risk managers should look to their organizations' traditional insurance policies as a source of potential coverage for cyber-related losses. *Spec's Fam. Partners, Ltd. v. Hanover Ins. Co.*, 17-20263, 2018 WL 3120794 (5th Cir. June 25, 2018) ("*Spec's Family*"); *Medidata Sols. Inc. v. Fed. Ins. Co.*, 17-2492, 2018 WL 3339245 (2d Cir. July 6, 2018) ("*Medidata*").

The *Spec's Family* Ruling

In *Spec's Family*, the U.S. Court of Appeals for the Fifth Circuit considered whether the trial court erred in granting judgment on the pleadings to the insurer. In the case, Spec's faced claims by its credit card processor demanding payment of amounts that the processor had to pay to reimburse issuing banks for costs associated with fraudulent transactions after Spec's credit card network was hacked. When Spec's sought defense coverage from Hanover under its management liability policy, the insurer asserted that the credit card processor's claims were barred from coverage based on a "breach of contract" exclusion, which precluded coverage for claims "directly or indirectly based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. However, this exclusion does not apply to your liability that would have attached in the absence of such contract or agreement." *Id*. at *2. The insurer claimed that this exclusion applied because Spec's potential liability arose out of a merchant agreement it had with the credit card processor, and the trial court agreed and granted judgment on the pleadings. On appeal, the Fifth Circuit, applying Texas law, reversed. The Fifth Circuit pointed to the broad duty to defend, stating that "[w]here an underlying petition includes allegations that 'go beyond' conduct covered by an exclusion, the duty to defend is still triggered." *Id*. at *4. The Fifth Circuit ruled that "[t]he pleadings, viewed in the light most favorable to Spec's, do not unequivocally show [the exclusion] excused Hanover's duty to defend under any set of facts or possible theory." *Id*. at *5. The court pointed, for example, to language in the credit card processor's claims that referred to "non-contractual theories of liability . . . , which must be construed in favor of Spec's and the duty to defend." *Id*.

The *Medidata* Ruling

In *Medidata*, the U.S. Court of Appeals for the Second Circuit considered whether a "spoofing" attack was covered under the computer fraud provision of a crime insurance policy. The provision covered losses stemming

from "entry of Data into" or "change to Data elements or program logic of" a computer system. *Id*. at *1. The insurer argued that this coverage applied only to hacking-type intrusions, and not instances where an email address had simply been disguised. Applying New York law, the Second Circuit rejected the insurer's argument and ruled that, although no hacking had occurred, "the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's email system," which indisputably constituted a "computer system" within the meaning of the policy. Because the spoofing code was introduced into the email system, the Second Circuit held that the attack was covered as "a fraudulent entry of data into the computer system." *Id*. at *1. The Second Circuit distinguished attacks where employees were simply duped by confusing email addresses, noting that the fraud against Medidata, by contrast, "clearly implicates the 'computer system qua computer system,' since Medidata's email system itself was compromised." *Id*. at *2.

The Takeaways

In addition to the fact that two prominent courts issued pro-policyholder rulings relating to cyber losses, there are several takeaways from these cases:

1. Never assume that cyber-related losses are not covered under traditional insurance policies. The management liability policy and the crime policy in the above cases are examples, but courts also have found coverage for cyber losses under first-party property policies and commercial general liability policies. Importantly, many companies faced significant business interruption losses last year from the WannaCry and NotPetya attacks, and there may be coverage for those losses under traditional property insurance policies.
2. In determining whether an insurer has a defense obligation, courts may broadly construe allegations of claims to find coverage. Even in instances where the gravamen or the vast majority of allegations in a claim or demand clearly fall within a policy exclusion, there still may be coverage so long as there are at least some allegations that are potentially outside the exclusion.
3. Insurers generally bear the consequences of ambiguous language. Under the law of most states, where policy language is not clear, the language will be construed against the insurer as the drafter and in favor of coverage. This "golden" rule means that policyholders should not take no for an answer and should challenge a denial where an insurer is relying on exclusionary language that is difficult to understand or inconsistent with the insured's reasonable expectations.
4. The process of reviewing insurance coverage for claims or losses can be difficult. Lowenstein Sandler's Insurance Recovery Group has been helping clients maximize recoveries for many years and is available to consult regarding strategies for conducting this review.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

ANDREW M. REIDY
Partner
T: 202.753.3752
areidy@lowenstein.com

JOSEPH M. SAKA
Counsel
T: 202.753.3758
jsaka@lowenstein.com

COURTNEY E. ALVAREZ
Counsel
T: 202.753.3760
calvarez@lowenstein.com