Lowenstein Sandler

Insurance Recovery

February 3, 2022

Subrogation Actions Following Ransomware Claims: What Policyholders Should Expect in the Ever-Changing Cyber Insurance Market

By Lynda A. Bennett and Michael J. Scales

Ransomware attacks continue to challenge U.S. companies, with cybercriminals now routinely extorting companies for multimillion-dollar payouts. A company that experiences an attack will likely seek coverage under its cyber insurance policy for any ransom it ultimately pays to the criminals and for the costs it incurs to restore its systems and retrieve its compromised data. The surge in ransomware attacks has resulted in insurers making frequent and substantial payments on these claims, to the point where the viability of the cyber insurance market is being stretched to its limits. As a result, we are seeing new trends emerge in terms of how insurers are responding to cyber claims: (1) They are taking more entrenched positions on claims payment, and (2) they are developing alternative mechanisms to minimize losses through subrogation actions. Policyholders need to be aware of these developments so that they can take steps before and after claims take place in order to preserve their rights and maximize coverage.

A case recently filed in the Northern District of California is a useful case study. In *Ace American Insurance Co. v. Accellion, Inc.*, N.D. Cal., Docket No. 21-cv-9615, Ace American Insurance Co. filed a subrogation action against Accellion, Inc., claiming the software company's negligence in handling a security vulnerability in its online file-transfer service led to a ransomware attack on its customer (and Ace's insured), a Boston law firm.

In its complaint, Ace alleges that Accellion became aware that its File Transfer Appliance (FTA) service, on which the law firm stored confidential files, contained a security vulnerability but failed to properly notify the law firm about the existence of the problem or a critical software update needed to fix it. Specifically, Ace alleges Accellion failed to inform the law firm of Accellion's internal client "notification" system used to inform its customer-users of security vulnerabilities and, when it did eventually send a notification to the law firm, it sent it to two employees who no longer worked there and then failed to follow up with the law firm to see whether anyone received the critical notification. Because the law firm never received the notification, Ace asserts, the law firm could not update its systems with the "fix" before hackers noticed the vulnerability and exploited it. The hackers stole confidential legal files and threatened to publicly disclose them unless the law firm paid millions of dollars. The law firm ultimately paid more than $2 million in ransom and thereafter filed a claim for the ransom and the costs it incurred to restore its files under its cyber policy issued by Ace. According to the complaint, when the law firm confronted Accellion about the security vulnerability, Accellion tried to shift the blame to the law firm, claiming the firm failed to update its contact information on Accellion's emergency notification system. Ace claims, however, that the law firm did all it could by notifying Accellion about its former employees' departures, and that it was Accellion's responsibility to update its own notification systems.

At the highest level, this case reflects a new trend in litigation stemming from the cyber insurance market. Faced with the reality that claims for ransomware attacks are substantial and prevalent and must be paid, insurers are seeking ways to offset their huge losses. As this case shows, insurers are trying to recoup their losses after claim payments by pursuing through subrogation the parties that are responsible for creating the opportunity for the security breach. If these subrogation actions "stick," policyholders should expect that once a cyber claim is paid by an insurer, that will not be the end of their involvement with responding to the breach. Rather, policyholders will be obligated under the terms of their policies to make their records, investigation results, and personnel available to the insurer as it pursues other potentially responsible parties. And that cooperation may not come without intangible cost to policyholders, especially if the source of the breach is a valued business partner. There are strategies that can be employed by policyholders to carefully navigate this sticky situation, and coverage counsel should be involved in that process.

Second, if these subrogation actions become a viable tool for insurers to recoup losses, policyholders can expect that insurers will take much greater interest at the underwriting stage with cyber policies in order to understand the terms and conditions of the policyholders' services contracts. To that end, policyholders will need to give much more intentional consideration to, and engage in negotiation of, insurance provisions in those services contracts.

Oftentimes, corporate lawyers drafting those provisions do not understand the nuances of insurance, including the importance of a "waiver of subrogation" clause that routinely is included in such provisions. This case identifies a significant risk that policyholders face if they have not aligned their services contract insurance provisions with their cyber policies and/or settlement agreements with insurers and other third parties, i.e., the policyholder may unwittingly **forfeit coverage** by violating the cooperation clause of its cyber policy if it broadly waives subrogation rights in a "standard" insurance provision in its services contract.

Third, service providers that have any interaction with the confidential information of other companies will be well advised to perform regular testing on the accuracy of their customer notification systems and evaluate their contingency plan to account for updates to customer contact information. As this case shows, following a ransomware attack, insurers responsible for paying the resulting insurance claim will be looking to hold third parties liable if their actions or failure to act allowed the attack to happen in the first place. Service providers should be diligent in their efforts to notify customers of security vulnerabilities and should follow up with them to ensure customers actually receive notifications of those vulnerabilities and act upon them.

Fourth, since a multitude of disputes between various parties will follow a ransomware attack, policyholders will be well advised to take precautionary security measures before an attack, and then document those measures and all communications and steps taken afterward. Unsurprisingly, after the law firm confronted Accellion following the attack, Accellion allegedly tried to shift the blame back onto the law firm, arguing that the law firm failed to update its notification system. Policyholders should expect the inevitable blame game and take all measures to avoid giving others any reason to pin responsibility on them. Policyholders should be transparent in their efforts and communicate those efforts to the insurer. This is consistent with the fundamental principle that policyholders should provide timely notice to their insurers, carefully investigate and document their claims, and consider all angles of an actual or potential liability before providing a release to any party associated with the loss.

Fifth, security breaches on a large scale have led to class actions brought by impacted parties pursuant to various privacy laws. Such lawsuits inevitably involve tremendous cost–both in terms of defending the action and eventually resolving it. In this case, Accellion was sued directly by its customers. However, if the law firm had been sued by its clients in connection with the breach, its insurer would have provided coverage to the firm for that action and then added those costs to the list of damages that it would seek from Accellion through the subrogation action. Thus, policyholders must keep in mind that security breaches are multifaceted and, following payment of a claim, the resulting subrogation action will address all angles of it.

Finally, this case highlights the fundamental importance of taking cybersecurity seriously and investing in it in the long run. Doing so will help businesses identify potential threats and vulnerabilities, not only in their own systems but also, as this case shows, in the systems of service providers with which the company shares confidential information that could be targeted in an attack. Policyholders can expect insurers to start requiring robust cyber protection for all entities that intersect with the confidential data that will be insured under the policy before coverage will be granted.

In sum, policyholders should expect that insurers will be more aggressive in the handling of cyber claims in the coming year, not only in terms of forcing policyholders to work harder to access their coverage in the first instance, but also after the claim has been paid by looking to recoup losses from third parties that are responsible for causing the security breach. Policyholders need to engage in active risk management before and after a loss occurs in order to ensure maximum recovery under their cyber policies.

Contacts

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

LYNDA A. BENNETT
Partner
Chair, Insurance Recovery
T: 973.597.6338
lbennett@lowenstein.com

MICHAEL J. SCALES
Associate
T: 973.422.6770
mscales@lowenstein.com