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

Del. Justices Clear Key Hurdle For Cyber Incident Recovery

By **Abraham Gross**

Law360 (March 5, 2026, 7:01 PM EST) -- A Delaware Supreme Court ruling allowed insurers to seek a collective recovery of their policyholders' losses from a ransomware attack, clearing a key procedural hurdle for policyholders and insurers to be made whole after a cyber incident.

The justices in their Feb. 13 ruling reversed the dismissal of two suits brought by insurance companies against Blackbaud Inc. after they determined the companies adequately pled a breach of contract claim for their policyholders, which insurance and cybersecurity experts flagged as potentially pivotal for future cyber incident recovery actions.

The court found that the insurers, including Travelers Casualty and Surety Co., could plead the claims of their policyholders in aggregate through a subrogation action, where insurers "stand in the shoes of the insureds" and seek to recoup their coverage payments.

The justices rejected Blackbaud's argument that aggregation disadvantaged the company, as well as the lower court's reliance on case law setting the standard that equitable-subrogation claims must identify each harmed party and could not aggregate distinct harms.

By contrast, the insurers in this case "identified each of the Insureds, the Blackbaud contract they had in common, the shared bases for the breaches, and the same or similar investigation and remediation damages incurred responding to the data breach," according to the opinion.

The justices also disagreed with the Superior Court's finding that the insurers did not adequately plead that Blackbaud's alleged breach was the proximate cause of harm.

They noted that the insurers pled that Blackbaud breached several security guarantees and shifted responsibility to clients, who incurred investigation and remediation costs.

Subrogation is becoming more common for cyber claims, in part as a reflection of the downstream affect of one vendor, said carrier-side attorney Matthew Bricker of Tittmann Weix.

"It's recognizing the systemic nature of modern cyber risk — just a single incident that's impacting many organizations — and so the courts are allowing them to be litigated in a practical way," he said.

Blackbaud provides software for managing donor relationships and information technology services for educational institutions and nonprofits.

The insurers paid more than $2.1 million collectively to their 97 insureds who were affected by a 2020 ransomware attack against Blackbaud's systems that accessed confidential customer data, according to court documents. At least some policyholders were subject to a retention, or out-of-pocket amount.

Policyholders often aren't made whole following a cyber coverage payout, said Rukesh Korde, a policyholder attorney for Covington & Burling LLP. In those cases, Korde said either the policies themselves or state law will explain how the proceeds from a subrogation suit will be divided between policyholders and their insurers.

"Oftentimes policyholders just don't have the resources to go after the responsible parties in these sorts of situations, but insurance companies do, and so this may provide a way for them to be made whole," he said.

Emily Garrison of Morgan Lewis' insurance recovery practice said that subrogations can present challenges over how recovered amounts are split and the order of payouts, and aggregate subrogation may raise the prospect that policyholders intervene to make sure their losses are given their due attention.

"There could be a potential concern that the carrier is not focusing as much as they should on my insurance recovery versus their global, universal recovery if it is going to be the case that they recover more than what they paid, and some of it comes back to the policyholder," she added.

Amy Mushahwar, chair of Lowenstein Sandler's data privacy, security, safety & risk management practice, told Law360 the decision should be a particular concern to companies that provide software as a service**.**

"Things that you do as a SaaS company to make it easier to service clients en masse, which is nearly identical contracts and nearly identical data flows that are impacted by breach and business flows, are the things that can be used against you in a ruling like this," she said.

The motion to dismiss stage is a crucial signal for settlements, and the ruling would likely provide leverage for insurers, who are more well-resourced than typical plaintiffs and have already had policyholders substantiate their claims for coverage, Mushahwar noted.

That added pressure could further strain vendors and their insurers, who may already be shouldering the costs of notifying clients, fixing issues and responding to regulatory investigations or investor suits.

In the case of the Blackbaud attack, the company has already paid a $3 million fine to the Securities and Exchange Commission over claims that its disclosures about the incident were misleading, a $49.5 million resolution of claims brought by states and the District of Columbia, and a separate $6.75 million deal with California.

The company also reached an agreement with the Federal Trade Commission to revamp its data security systems and practices, and entered into confidential settlement agreement last July to resolve claims brought by individual plaintiffs that their personal data was compromised.

"Will there be a world where Blackboard or any SaaS client will actually have to insure such that they are

shouldering the cost of not just their losses, but the losses of every single underlying company underneath them?" Mushahwar said. "That could become prohibitively expensive for SaaS companies to serve mass client bases."

Bricker of TittmannWeix LLP noted that the Blackbaud case still in its early stage, and that other coverage-related issues remain to be sorted, including liability caps, limits on consequential or other damages, and determining if the alleged conduct was gross negligence or intentional conduct, which is typically excluded.

Vendors may respond to the ruling by modifying contracts to limit their liability or the potential for subrogation, in addition to mitigating their risks technologically so that incidents are less disruptive across clients and their operations, Mushahwar said.

Insurers, in turn, would likely place a greater focus on those very contract provisions, said Garrison of Morgan Lewis.

"I could see insurers doing more underwriting diligence in terms of what your service provider contracts provide, knowing that that may be a source of recovery down the road if there's an incident," she told Law360.

The Delaware Supreme Court remanded the case back to Delaware Superior Court.

The cases are Travelers Casualty and Surety Co. of America et al. v. Blackbaud Inc., case numbers 193, 2025 and 198, 2025, in the Delaware Supreme Court.

--Additional reporting by Rae Ann Varona, Ganesh Setty, Elizabeth Daley and Allison Grande. Editing by Amy Rowe and Nick Petruncio.
