New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
ALM.
VOLUME 268—NO. 63
THURSDAY, SEPTEMBER 29, 2022

Outside Counsel

Guidance for Companies Facing Class Actions Post-'TransUnion'

BY WILLIAM RIDGWAY, MEREDITH SLAWE AND RACHEL CHENG

Even as ransomware demands skyrocket in price, businesses continue to pay their attackers hoping to restore their operations and prevent the leak of sensitive customer or employee data. Indeed, one recent study reported that over half of surveyed ransomware victims opted to make these payments. But paying the ransom seldom ends the ordeal for companies as they often become targets for class action litigation, particularly when the attackers manage to steal sensitive customer or employee data.

Photo: Thodonal via Adobe Stock

Nevertheless, the Supreme Court's decision in *TransUnion* may provide a pathway for ending that litigation early if the ransom is paid to prevent data leakage. Below we explain how companies can seize upon that case law to position themselves for a favorable outcome in litigation.

A New Standing Regime Under 'TransUnion'

In *TransUnion v. Ramirez*, the U.S. Supreme Court held that a majority of the members of a class asserting claims under the Fair Credit Reporting Act lacked Article III standing. Those class members lacked standing to complain about credit reports misidentifying them as potential terrorists or serious criminals because they could not show that those errors were disseminated to third parties.

Although class members were exposed to the risk of future

WILLIAM RIDGWAY *is a litigation partner at Skadden, Arps, Slate, Meagher & Flom and a former federal prosecutor. He is an experienced trial and appellate lawyer whose practice focuses on white collar crime, cybersecurity, data privacy and national security matters and complex civil litigation.* MEREDITH SLAWE *is a litigation partner at the firm and represents clients across a range of industries in class actions nationwide and mass arbitrations.* RACHEL CHENG *is a litigation associate at the firm.*

harm by the inaccurate information contained in their files, there was no "concrete" harm without publication. In so holding, the court reiterated that a plaintiff alleging intangible injury must show "a close relationship" between that harm and an injury traditionally recognized as grounds for a lawsuit."

TransUnion promises to carry significant implications for consumer class actions and provide an avenue for companies that pay the ransom to exit from resultant litigation in earlier stages. In a typical ransomware attack, hackers steal sensitive customer or employee data before encrypting the company's system. The data theft is then used to put more pressure on the victim to pay. In addition to withholding the decryption key, the attackers will threaten to leak the stolen data on the dark web if they do not receive payment. Thus, paying the ransom—and thereby retrieving the stolen data—may prevent the company's customers or employees from experiencing a concrete injury under *TransUnion*.

A recent court decision entertained this theory. In *In re Practicefirst Data Breach Litigation*, a district court dismissed on standing grounds a class action against a medical management company that suffered a ransomware attack and data breach. Notably, in that case the company retrieved the stolen data, presumably by paying the ransom. The court concluded that the plaintiffs failed to allege an imminent risk of future harm or a concrete injury and thus fell short of the *TransUnion* standard.

'TransUnion' promises to carry significant implications for consumer class actions and provide an avenue for companies that pay the ransom to exit from resultant litigation in earlier stages.

In the court's view, it was not enough that the plaintiffs claimed to face an ongoing and increased risk of identity theft or fraud and to have devoted time protecting themselves against identity theft. The court noted the company's retrieval of the stolen data (a fact plaintiffs appeared to concede) contributed to its conclusion that the plaintiffs failed to plausibly allege the data breach was a targeted attempt to expose the plaintiffs to identity theft or another similar form of fraud.

Not every class action will be susceptible to dismissal at the motion to dismiss stage—in part because plaintiffs have proven adept at pleading around these issues—but *TransUnion*'s reasoning should also bear on whether to certify a class, a key decision that determines the stakes of a case. By raising the bar for standing in the class-action context, *TransUnion* offers a powerful argument that standing is a threshold constitutional requirement that applies to individual class members just as it would to individual litigants, and that it should therefore be addressed and resolved at the earliest practicable point in the case, including before certifying a class, especially when there are good signs that not everyone in the class is injured.

Practical Guidance for Paying the Ransom

As a threshold matter, companies need to be aware that the Treasury Department requires ransomware victims and their financial institutions to perform due diligence on those to whom they plan to pay ransom.

Because several prolific ransomware groups are subject to U.S. sanctions, Treasury rules may prohibit some ransom payments. That leaves the victims with no choice but to rebuild their systems from scratch and suffer the consequences of having their data disclosed publicly. If it is permissible to pay the ransom and a company decides to do so, here are steps it can take to improve their odds in litigation at dismissal or defeating class certification by retrieving stolen data in a manner that will be upheld in court:

Use experienced ransomware negotiators to engage with threat actors. There are third-party experts that have experience negotiating with ransomware threat actors. Once engaged, these negotiators will communicate with the threat actors on behalf of the company. Negotiators may use their previous experience to assess the actor's reliability, considering factors such as whether the ransomware group has historically decrypted systems after receiving payment. This expertise and evaluation can be critical to determining whether threat actors will make good on their promises to retrieve and delete the data after payment.

Prioritize discussion of data retrieval in any negotiation. If a company is considering a ransomware payment, it should discuss (through its negotiator) with threat actors how they propose to assure data retrieval. Ideally the threat actors will provide written confirmation of these logistics, including where the stolen data is stored.

By raising the bar for standing in the class-action context, 'TransUnion' offers a powerful argument that standing is a threshold constitutional requirement that applies to individual class members just as it would to individual litigants

Trace back the stolen data. If the threat actors disclose where the data is being stored, companies should determine if it matches the location for the original data exfiltration. If there is a discrepancy, companies should insist on deletion from all locations and require evidence that the data does not reside on any other location. Taking these steps can help prevent the risk that the threat actors will demand a second ransom payment, claiming to have access to data that has already been ransomed.

Generate reliable evidence of data deletion. Companies should request the ability to delete the data themselves. In that case its forensic provider or ransomware negotiator can access the system and clearly document the deletion of the data in a manner that would be admissible in court. If the threat actors do not allow that, companies should still insist on documented evidence of data deletion.