CARLTON FIELDS

# Ransomware Attacks and Class Action Litigation: A Two-Headed Monster

July 26, 2021

High-profile ransomware attacks have dominated the headlines this year. Those attacks pose existential threats for some victim companies, and they also may garner the attention of regulators. In addition, these attacks are increasingly prompting the filing of class action lawsuits. This means that the victim company not only must withstand the attack itself, but also faces litigation exposure. This article documents this phenomenon and provides practical suggestions and resources to mitigate these risks.

## The Rise of Ransomware

Ransomware attacks exploded during the pandemic and have continued unabated. According to the federal government, attackers received approximately $350 million in ransom payments in 2020, an increase of more than 300% from 2019. Those attacks have targeted businesses and organizations in virtually every sector. Further, those attacks often target small and medium-sized businesses.

Meanwhile, ransomware attacks have evolved beyond locking up a victim's networks and systems to also, in many cases, stealing the victim's data. The attacker then threatens to disclose that data publicly unless the ransom is paid.

## Class Actions to Follow

Increasingly, a ransomware attack — particularly if it involves the theft of victim data that includes customer or employee information — prompts the filing of one or more class actions. In such an action, the plaintiffs assert that the victim should have done more to prevent the attack and the theft of data.

The increased risk of class actions in the wake of a ransomware attack aligns with the findings of the *2021 Carlton Fields Class Action Survey*, which draws on 415 interviews of general counsel and

senior legal officers at major corporations regarding class action trends. Survey respondents predicted that the next wave of class actions would stem from cybersecurity issues and data privacy, including ransomware attacks.

Further, plaintiffs may use these class actions to pursue novel theories of liability. For example, pipeline operator Colonial, which experienced a ransomware attack in May, faces two class actions brought by consumers and gas station owners, respectively. Those claims don't seek relief based on compromised personal data; rather, they assert that Colonial's negligence caused higher gasoline prices.

## What to Do

Whether the Colonial plaintiffs will succeed will turn on several issues, including the reasonableness of Colonial's cybersecurity measures, policies, and procedures. "Reasonable security" is a frequently used term in cybersecurity but is often undefined.

Given the ambiguity in that term, plaintiffs may argue that a defendant company failed to avail itself of publicly available resources that allegedly could have thwarted the attack. Indeed, the Colonial plaintiffs cite various government resources and pronouncements regarding ransomware. And, with the spike in ransomware, those publicly available resources are growing.

One such resource is the recently unveiled government website StopRansomware.gov. This website contains an array of resources, including articles describing ransomware, providing tips for protecting an organization, recommendations for responding to an attack, and links for reporting an attack.

The government's release of this website comes on the heels of ransomware guidance issued by the White House in June, as well as guidance issued by other regulators, including the New York State Department of Financial Services.

The government's ransomware website and these other government resources offer practical suggestions for mitigating the chance of an attack in the first place and, should an attack occur, helping the company to respond quickly. Those resources identify several measures to promote "cyber hygiene" and reduce risk, including:

- Email filtering and anti-phishing training
- Vulnerability/patch management
- Multifactor authentication
- Strong password management

- Privileged access management
- System monitoring and response solutions
- Developing and testing an incident response plan

In addition to checking the extent to which these measures are in place, companies should (i) review their insurance program, including any cyber insurance policies; and (ii) develop a compliance program to evaluate the sanctions risk posed by paying a ransom. Item (ii) is particularly important in light of the government's position that paying a ransom may expose a victim company to a sanctions enforcement proceeding.

In the end, the risk of ransomware is likely here to stay. The risk of an attack is further compounded by the increased likelihood of litigation, including class actions, in the wake of such an attack. Faced with that landscape, companies should leverage the aforementioned resources wherever possible.

## Related Practices

Cybersecurity and Privacy
Technology

## Related Industries

Technology