wiley

ALERT

Ransomware Attacker Files SEC Complaint to Increase Pressure on Victim

November 17, 2023

The Black Cat/ALPHV ransomware group filed a complaint with the U.S. Securities and Exchange Commission (SEC) to allege that one of their victims failed to disclose a cyberattack to the SEC within four days, reports Bleeping Computer. Yes, that's right, a ransomware group apparently tried to leverage the SEC's new public cyber disclosure rule to extort a victim company. We sympathize with the victim company and are skeptical of all cyberattacker claims, but we are troubled by the apparent abuse of regulatory process, particularly as new cyber requirements proliferate.

Black Cat reportedly listed the software company MeridianLink, Inc. on their data leak site with a threat that they would leak allegedly stolen data unless the ransom is paid in 24 hours. MeridianLink is a publicly traded company that provides digital solutions for financial organizations such as banks, credit unions, and mortgage lenders.

When MeridianLink allegedly didn't respond to ransom demands, Black Cat attempted to exert more pressure on the company by sending a complaint to the SEC about the company for allegedly not disclosing a cybersecurity incident that impacted customer data and operational information. Entitled "MeridianLink fails to file with the SEC..so we do it for them + 24 hours to pay," the ransom group wrote:

> *The recent adoption of SEC rules mandates public companies to promptly disclose material cybersecurity incidents under Item 1.05 of Form 8-K within four business days of determining such incidents to be material. Despite this requirement, MeridianLink has not fulfilled this obligation regarding the breach it experienced a week ago. We have there fore reported this non-compliance by MeridianLink, who was involved in a material*

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

Securities Enforcement and Litigation

> *breach impacting customer data and operational information, for failure to file the required disclosure with the Securities and Exchange Commission.... [W]e are giving you 24 hours before we publish the data in its entirety.*

To try to show that their complaint to the SEC was real, Black Cat published a screenshot of the form they filled out on the SEC's Tips, Complaints, and Referrals page. The group also reportedly published the response it received from the SEC thanking the group for contacting the SEC and acknowledging that its response had been received successfully.

Regardless of the veracity of the underlying claims by Black Cat, the move is troubling. Ransomware actors frequently use the threat of publicly reporting data breaches as a way to extort payments from victim companies, but this appears to be the first time a group tried to leverage the SEC's rules to facilitate extortion.

The SEC's new cybersecurity rules are set to take effect on December 15, 2023, and require disclosure of cybersecurity incidents "four business days after a registrant determines that a cybersecurity incident is material." SEC requirements previously expected general reporting of material adverse events, but the new rule adds more requirements and sets a rigid clock for reports. It also adds to some confusion about what events will be seen as "material."

Industry pushed back hard on the SEC's proposals. Commenters across the economy warned about early disclosures leading to potential revictimization of companies, and argued that the new rules were too rigid and would pressure or compromise ongoing forensic and law enforcement investigations. After the SEC largely dismissed those concerns in the final rule, the agency and the FBI are defending the rules and trying to give the private sector comfort that the rules won't lead to security risks or overburden them.

But, this troubling development shows that government reporting obligations can have unintended results. The exploitation of the SEC's rules to pressure a victim company into paying ransom after a real or alleged cyber incident is a worrisome unintended consequence of the new SEC cyber disclosure rules. Hopefully the SEC rejects the criminals' attempt to misuse government in its criminal enterprise, and stands up for victims.