Hackers Turned Whistleblowers: SEC Cybersecurity Rules Weaponized Over Ransom Threat

November 20, 2023

On November 7, 2023, the profilic ransomware group AlphV (a/k/a "BlackCat") reportedly breached software company MeridianLink's information systems, exfiltrated data and demanded payment in exchange for not publicly releasing the stolen data. While this type of cybersecurity incident has become increasingly common, the threat actor's next move was less predictable. AlphV filed a whistleblower tip with the U.S. Securities and Exchange Commission (the "SEC") against its victim for failing to publicly disclose the cybersecurity incident. AlphV wrote in its complaint:[1]

> We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules. It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

As we have previously reported, the SEC adopted final rules mandating disclosure of cybersecurity risk, strategy and governance, as well as material cybersecurity incidents. This includes new Item 1.05 of Form 8-K, which, beginning December 18, will require registrants to disclose certain information about a material cybersecurity incident within four business days of determining that a cybersecurity incident it has experienced is material. Though AlphV jumped the gun on the applicability of new Item 1.05, its familiarity with, and exploitation of their target's public disclosure obligations is a further escalation in a steadily increasing trend of pressure tactics by leading ransom groups.

[1] A copy of the submission was shared by the threat actor with DataBreaches on November 15, 2023 and is available here.

WHY WOULD A THREAT ACTOR BLOW THE WHISTLE ON THEIR OWN CRIME?

The percentage of companies that now make extortion payments to recover access to encrypted systems or stop stolen data from being posted publicly is on the decline.[2] Threat actors are accordingly resorting to increasingly aggressive harassment techniques to extract such payments from victims. This move is an extension of those aggressive pressure tactics. Large threat groups, like BlackCat/AlphV, are sophisticated and aware of regulatory, financial and other company pressures, and have in the past threatened to alert regulators or otherwise have taken to social media or other public outlets to pressure victims to pay. In this instance, the threat actor is attempting specifically to leverage the SEC's regulations to its advantage by increasing the cost to their targets of refusing to pay ransom– namely, by increasing the likelihood that the regulator will investigate the cybercrime victim, which can be incredibly costly, time consuming and damaging to a company's reputation and business.

HOW WILL THE SEC RESPOND?

Unsurprisingly, the SEC has not yet issued a statement regarding the AlphV whistleblowing complaint, and it is not yet clear how the SEC will handle whistleblower complaints by threat actors. However, this move could arguably result in an increase in the filing of such whistleblower tips by such threat actors and, accordingly, could more generally trigger increased investigative scrutiny into companies that fall victim to cybercrime, including investigations of whether their public disclosures or disclosure controls were deficient in connection with the cybersecurity incident. This will become increasingly true as the new rules come into effect and require timely disclosure of material cybersecurity incidents.

WILL THE THREAT ACTOR BE ENTITLED TO A WHISTLEBLOWER AWARD UNDER THE SEC'S RULES?

Probably not. Rules 21F-6 and 21F-16 under the Securities Exchange Act of 1934 provide for a reduction in whistleblower awards based on culpability and other factors, assuming that there is an enforcement action resulting from the tip exceeding $1 million in monetary remedies.

In any event, to be eligible for payment, a whistleblower must be a natural person and must disclose their identity on form WB-APP. (This would be true even if the applicant initially submitted their complaint on an anonymous basis. *See* §§ 240.21F-7(b) and

[2] *Ransom Monetization Rates Fall to Record Low Despite Jump in Average Ransom Payments*, COVEWARE (July 21, 2023), https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments.

240.21F-10(c).) As such, even if a threat actor were otherwise entitled to an award as a matter of law, the procedural requirements for recovery make it unlikely that they would ever seek payment, given their interest in avoiding personal liability for the underlying criminal conduct. Therefore, it is less likely that a threat actor would file a complaint with the hope of recovering an award and more likely that they would view the filing simply as further means of supporting their extortion of current and future victims.

HOW SHOULD PUBLIC COMPANIES PREPARE TO RESPOND?

Stand by your disclosure controls and materiality determination, and be prepared to respond to regulators, customers and other stakeholders from a crisis communications standpoint. With the compliance date for the new SEC cybersecurity rules looming, public companies should ensure their cybersecurity incident response plan and disclosure controls and procedures are ready. Documenting a thorough and deliberative materiality determination, at each point in a cybersecurity incident response at which significant new facts become available, will be of paramount importance to support Item 1.05 disclosure decisions. Lowering the bar for Item 1.05 disclosure—or, worse, paying a ransom in response to this type of threat—will ultimately set a dangerous precedent for future 8-K disclosures.

For more information about the SEC's cybersecurity rules, see our prior updates:

- SEC Adopts New Cybersecurity Rules for Issuers
- SEC Adopts New Cybersecurity Rules for Issuers – Part 2 Key Takeaways.

We will continue to monitor developments in this area.

To subscribe to the Data Blog of our Data Strategy and Security practice, please click here.

* * *

Please do not hesitate to contact us with any questions.

Andrew J. Ceresney
Partner, New York
+1 212 909 6947
aceresney@debevoise.com

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar @debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

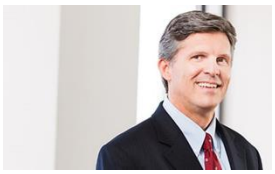
Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Matthew E. Kaplan
Partner, New York
+1 212 909 7334
mekaplan@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Benjamin R. Pedersen
Partner, New York
+1 212 909 6121
brpedersen@debevoise.com

Steven J. Slutzky
Partner, New York
+1 212 909 6036
sjslutzky@debevoise.com



Jonathan R. Tuttle
Partner, Washington, D.C.
+1 202 383 8124
jrtuttle@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Kelly Donoghue
Associate, New York
+1 212 909 6145
kgdonoghue @debevoise.com