If at first you don't succeed, screw it up again? - DataBreaches.Net

Published: 2023-12-18 · Archived: 2026-04-09 02:20:45 UTC

In mid-November, DataBreaches reported that AlphV threat actors had added MeridianLink to their leak site. When their victim wouldn't pay them, AlphV (aka "BlackCat") filed a complaint with the Securities & Exchange Commission alleging that MeridianLink failed to comply with the SEC's new cybersecurity rule requiring notification within four days of discovering a material breach.

Unfortunately for AlphV, they did not seem to know that the law wasn't in effect yet.

Today, BlackCat tried again. Their leak site now lists **Viking Therapeutics** as a victim. Instead of providing any proof of claims, however, they posted that they got (translated: intimidated) a Viking Therapeutics (VT) employee to file an SEC report on his own company:

> Despite the stringent cybersecurity disclosure requirements set forth by the Securities and Exchange Commission (SEC), Viking Therapeutics failed to promptly report a material cybersecurity incident involving patient data as mandated. To address the new criteria for a persons reporting an incident, an employee of Viking Therapeutics has agreed to file a report after a productive talk with his family. Complaint details are below:

The employee's complaint alleges that the firm violated the 4-day reporting deadline, stating in relevant part:

> I hope this message finds you well. I am writing to bring to your attention a matter of significant concern regarding the failure of our company, Viking Therapeutics, to file a required cybersecurity incident report within the stipulated timeframe. As an employee deeply committed to compliance and transparency, I feel obligated to inform you that Viking Therapeutics has not fulfilled its obligation to report a material cybersecurity incident involving patient data. This omission is particularly alarming considering the potential impact on our stakeholders and investors. The incident in question involves a breach of patient data, which, to my knowledge, constitutes material information.

If AlphV's post is truthful in claiming that an employee filed the complaint, it appears to have been under duress.

AlphV also claims that the incident has already been reported to HHS:

> As it is unlikely that this organization will notify the HHS in regards to the breach of patient data, within the 60 days time-frame, we have already done so. In the event we do not receive contact within 48 hours, the data will be published in its' entirety. After closer examination of the data, the SEC has also been informed regarding the misleading of investors due to discrepancies in published trial outcomes to shareholders

According to the affiliate involved in this incident, the attack occurred six days ago. But when DataBreaches later requested proof of receipt from the SEC and asked for clarification as to what AlphV was calling a misleading discrepancy in published trial outcomes, there were no replies.

Once again, the attempt to invoke the SEC cybersecurity reporting rule fails, as the rule first went into effect today. As Hunton Andrews Kurth explains (emphasis added by DataBreaches):

> … the U.S. Securities and Exchange Commission's ("SEC") new Form 8-K rules for reporting material cybersecurity incidents take effect today, December 18, for filers other than smaller reporting companies. The new rules require reporting to the SEC within four business days from the determination of materiality.
>
> […]
>
> **Compliance Dates.** The Form 8-K and 6-K reporting requirement will take effect for **cyber incidents occurring on or after December 18, 2023, though smaller reporting companies will have a delay until June 15, 2024**. These dates may slip further if there is any undue delay in publishing the final rules in the Federal Register. The annual reporting requirement on Form 10-K or 20-F will take effect for fiscal years ending on or after December 15, 2023. Thus, annual reports published in 2024 will generally require the inclusion of the new Item 106 disclosure.

Whether the Viking Therapeutics employee knew there was no requirement to report this incident to the SEC but was just so scared that they submitted it, or whether AlphV's claims are just total lies is unknown to DataBreaches.

DataBreaches did reach out to Viking Therapeutics, sending an email inquiry to a few of their executives. The email was clear that DataBreaches knows they had no obligation to report to the SEC under the new rule, but asked what they were doing in response to the alleged incident.

No reply has been received.

DataBreaches made no attempt to contact HHS at this time.

So far, then, all we have is an unconfirmed alleged breach.

DataBreaches will update this post if more information becomes available.
