

An Update on the SEC's Cybersecurity Reporting Rules

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

As we pass the two-month anniversary of the effectiveness of the U.S. Securities and Exchange Commission's ("SEC's") [Form 8-K cybersecurity reporting rules](#) under new Item 1.05, this blog post provides a high-level summary of the filings made to date.

Six companies have now made Item 1.05 Form 8-K filings. Three of these companies also have amended their first Form 8-K filings to provide additional detail regarding subsequent events. The remainder of the filings seem self-contained such that no amendment is necessary, but these companies may amend at a later date. In general, the descriptions of the cybersecurity incidents have been written at a high level and track the requirements of the new rules without much elaboration. It is interesting, but perhaps coincidental, that the filings seem limited to two broad industry groups: technology and financial services. In particular, two of the companies are bank holding companies.

Although several companies have now made reports under the new rules, the sample space may still be too small to draw any firm conclusions or decree what is "market." That said, several of the companies that have filed an 8-K under Item 1.05 have described incidents and circumstances that do not seem to be financially material to the particular companies. We are aware of companies that have made materiality determinations in the past on the basis of non-financial qualitative factors when impacts of a cyber incident are otherwise quantitatively immaterial, but these situations are more the exception than the rule.

There is also a great deal of variability among the forward-looking statement disclaimers that the companies have included in the filings in terms of specificity and detail. Such a disclaimer is not required in a Form 8-K, but every company to file under Item 1.05 to date has included one. We believe this practice will continue.

Since the effectiveness of the new rules, a handful of companies have filed Form 8-K filings to describe cybersecurity incidents under Item 8.01 ("Other Events") instead of Item 1.05. These filings have approximated the detail of what is required under Item 1.05. It is not immediately evident why these companies chose Item 8.01, but presumably the companies determined that the events were immaterial such that no filing under Item 1.05 was necessary at the time of filing. Of course, the SEC filing is one piece of a much larger puzzle when a company is working through a cyber incident and related remediation. It remains to be seen how widespread this practice will become. To date, the SEC staff has not publicly released any comment letters critiquing any Form 8-K cyber filing under

the new rules, but it is still early in the process. The SEC staff usually (but not always) makes its comment letters and company responses to those comment letters public on the SEC's EDGAR website no sooner than 20 business days after it has completed its review. With many public companies now also making the new Form 10-K disclosure on cybersecurity, we anticipate the staff will be active in providing guidance and commentary on cybersecurity disclosures in the coming year.

Copyright © 2025, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume XIV, Number 56

Source URL: <https://natlawreview.com/article/update-secs-cybersecurity-reporting-rules>