Lessons Learned: One Year of Form 8-K Material Cybersecurity Incident Reporting

February 11, 2025

On December 18, 2023, the Securities and Exchange Commission's (the "SEC") rule requiring disclosure of material cybersecurity incidents became effective. To date, 26 companies have reported a cybersecurity incident under the new Item 1.05 of Form 8-K ("Item 1.05"). After over a year of mandatory cybersecurity incident reporting, we examine the key trends and takeaways.

Key Takeaways from a Year of Cybersecurity Incident Reporting on Form 8-K

In early 2024, companies filed a flurry of Forms 8-K under Item 1.05, which stated that the relevant cybersecurity incidents did not have material impacts on the companies' financial conditions or results of operations. These disclosures were in response to the SEC's rules requiring that cybersecurity incident disclosures include a description of "the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the issuer, including its financial condition and results of operations." Following these disclosures, the SEC clarified its expectations for cybersecurity incident reporting in a statement issued by the Director of the SEC's Division of Corporation Finance (the "Statement"), as well as through several comment letters issued by the Staff of the SEC (the "Staff") to companies which filed Item 1.05 Forms 8-K.

Disclosing Nonmaterial Cybersecurity Incidents Under Item 8.01 of Form 8-K

The Statement, released on May 21, 2024, discouraged the use of Item 1.05 for voluntary disclosure of immaterial incidents: "[a]lthough the text of Item 1.05 does not expressly prohibit voluntary filings, Item 1.05 was added to Form 8-K to require the disclosure of a cybersecurity incident 'that is determined by the registrant to be material,' and, in fact, the item is titled 'Material Cybersecurity Incidents.'" The Statement clarified the SEC's views on when and how registrants should disclose cybersecurity incidents:

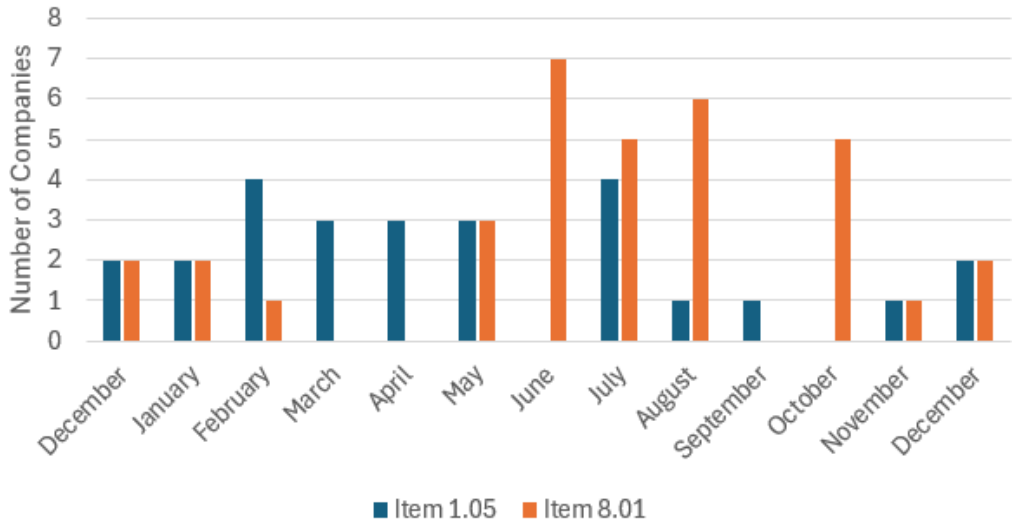
- Where a registrant voluntarily discloses an incident that is not material, or that the registrant has not yet determined to be material, the Division of Corporation Finance encourages the company to disclose that cybersecurity incident under a different item of Form 8-K (for example, Item 8.01) rather than under Item 1.05.

- If a registrant has previously voluntarily disclosed an immaterial incident (or one for which it had not yet made a materiality determination), and it subsequently determines that the incident is material, the registrant should file an Item 1.05 Form 8-K within four business days of such materiality determination.

- If an incident is so significant that a registrant determines it to be material, even though the registrant has not yet determined the scope of its impact, a registrant should file under Item 1.05 to provide investors with information about the material aspects of the incident and later amend the Form 8-K to disclose the material impacts once that information is available.

The Statement also reminded companies that, when determining whether a cybersecurity incident is material, the registrant should assess "all relevant factors," which are not "limited to the incident's impact on the company's financial condition and results of operation." The Statement emphasized that registrants should consider qualitative factors alongside quantitative factors, including harm to reputation, customer or vendor relationships or competitiveness, and the possibility of litigation or regulatory investigations or actions.

Form 8-K Cybersecurity Filings under Item 1.05 vs. Item 8.01 since December 18, 2023



The pace of disclosure of cybersecurity incidents under both Item 1.05 and Item 8.01 was markedly different in the months following the Statement. Whereas 17 companies

disclosed cybersecurity incidents under Item 1.05 prior to the Statement, nine companies disclosed cybersecurity incidents under Item 1.05 following the Statement (through the end of 2024). On the other hand, we observed an increase in cybersecurity incidents disclosed under Item 8.01 following the Statement. During 2024, six companies disclosed cybersecurity incidents under Item 8.01 prior to the Statement, whereas 28 companies disclosed cybersecurity incidents under Item 8.01 following the Statement.

Of the 26 companies that have filed Forms 8-K to report a cybersecurity incident under Item 1.05, seven identified a material impact in their initial filings and another two identified a material impact in subsequent amended filings. Of those seven companies that identified a material impact in their initial filings, the majority (five) were filed following the Statement, similar to the trend observed in the overall number of Item 1.05 and Item 8.01 filings.

In light of the SEC's guidance, companies should reserve the use of Item 1.05 for cybersecurity incidents that they determine have had, or are reasonably likely to have, a material impact on their business. Where companies wish to voluntarily disclose a cybersecurity incident that they have not determined to be material, they should disclose the incident through a different means, such as Item 8.01, press release, or other investor communication.

Clarifying the Purpose of Item 1.05: SEC Comment Letters

On January 5, 2024, the Staff issued its first comment letter in respect of the new disclosure requirements, responding to V.F. Corporation's Item 1.05 Form 8-K filed on December 15, 2023. The Staff cited V.F. Corporation's disclosure that "the full scope, nature and impact of the incident are not yet known" and that "[t]he Company has not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations." In its letter, the Staff requested that V.F. Corporation file a Form 8-K amendment, commenting that V.F. Corporation should "expand [its] discussion to describe the scope of [its] business operations impacted … describe the known material impact(s) the incident has had and the material impact(s) that are likely to continue" and "[i]n considering material impacts … describe all material impacts." The comment letter referred to vendor relationships and reputational harm as examples of potentially material impacts.

These early comments from the Staff served as a reminder to companies to provide meaningful disclosure and actively monitor the status of cybersecurity incidents for potential updates, especially when significant information is unknown at the time of the initial filing. V.F. Corporation filed a Form 8-K amendment on January 18, 2024, disclosing additional information about the scope, nature and impact of the

cybersecurity incident. Notably, however, the Form 8-K amendment did not disclose any additional material impacts of the cybersecurity incident.

Between May 24 and July 26, 2024, the SEC conducted a "sweep" review of Item 1.05 Forms 8-K, issuing 14 comment letters that focused on (i) the choice to disclose under Item 1.05 if the incident was not material or had not yet been determined to be material and (ii) expanding disclosure about potential material impacts beyond financial condition and results of operations.

For example, on July 26, 2024, the Staff issued a comment letter to AT&T Inc. in respect of its Item 1.05 Form 8-K filed on July 12, 2024 and, following AT&T Inc.'s response on July 31, 2024, a clearance letter issued on August 19, 2024. The Form 8-K disclosed that AT&T had experienced a cybersecurity incident in which hackers accessed and stole phone and SMS records for nearly all of AT&T's customers, including personal, business, and government accounts. AT&T disclosed that it had "not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations."

In its comment letter, the Staff questioned AT&T's choice to disclose the incident under Item 1.05, given that AT&T had not yet determined the materiality of the incident. The Staff also requested that AT&T file a Form 8-K amendment, commenting that AT&T should "provide a more detailed description of the nature and scope of the incident, including the types of data compromised, the number and categories of customers affected, the duration of the unauthorized access, and the methods used by the hackers" and that AT&T should "discuss the material impact or reasonably likely material impact of the incident on the Company, including its financial condition and results of operations, as well as any other material impacts, such as legal, regulatory, reputational, operational, or competitive risks or consequences." In the uncharacteristically lengthy clearance letter, the Staff further disagreed with AT&T's position that an incident could be "material" (thus triggering Item 1.05 disclosure) without having any disclosable material impacts. The Staff's correspondence with AT&T reinforces its position that disclosure under Item 1.05 should be exclusively reserved for cybersecurity incidents that companies determined have had, or are reasonably likely to have, a material impact on their business and that all such material impacts must be described.

What Can We Learn from Recent Enforcement Actions

Although the SEC has not yet brought an enforcement action relating to the new disclosure rules, they have brought several actions relating to pre-Item 1.05 disclosures, including a December 2024 case involving Flagstar Bancorp, Inc. ("Flagstar") relating to a cybersecurity incident in 2021. In January 2021, Flagstar suffered a cyberattack that disrupted its online and mobile banking services for several days, affecting over a

million customers. Flagstar filed a Form 8-K under Item 8.01 on January 25, 2021, disclosing the incident and stating that it had "no evidence of unauthorized access to customer information or impact to the security of customer accounts." However, the SEC alleged that Flagstar's disclosure was false and misleading, as the company had learned on January 24, 2021 that the attackers had accessed and exfiltrated sensitive customer data, including names, addresses, social security numbers, account numbers and balances. Flagstar amended its Form 8-K and disclosed the data breach on February 9, 2021, after it had notified the affected customers.

On December 16, 2024, the SEC settled with Flagstar, finding that Flagstar violated Section 13(a) of the Securities Exchange Act of 1934 and Rule 13a-11 thereunder, which require issuers to file accurate current reports on Form 8-K. The SEC also found that Flagstar violated Sections 17(a)(2) and (3) of the Securities Act of 1933, which prohibit issuers from obtaining money or property by means of any untrue statement of a material fact or any omission to state a material fact, or engaging in any transaction, practice or course of business that operates or would operate as a fraud or deceit upon the purchaser. In addition, the SEC found that, in violation of Rule 13a-15 under the Securities Exchange Act of 1934, Flagstar failed to maintain disclosure controls and procedures regarding cybersecurity incidents designed to ensure that relevant information to assess materiality was considered by disclosure decision-makers. Flagstar agreed to settle the charges without admitting or denying the findings and consented to a cease-and-desist order and a civil penalty of $3.5 million.

The Flagstar case illustrates the importance of both timely and accurate disclosure of cybersecurity incidents under the SEC's rules and maintenance of robust disclosure controls and procedures to address disclosure of cybersecurity incidents. In particular, the order highlighted the SEC's finding that, while Flagstar's disclosure decision-makers received regular updates about an incident, "Flagstar's cybersecurity procedures and controls lacked guidance on what factors to consider in assessing materiality for purposes of disclosure, which disclosure decision makers were responsible for making the materiality assessment, and how that assessment was to be documented and/or communicated to management."

The recent SEC enforcement action against SolarWinds Corp. further complicates the SEC's enforcement landscape regarding cybersecurity protocols. On July 18, 2024, U.S. District Judge Paul Engelmayer dismissed the majority of the SEC's claims against SolarWinds, including the novel assertion that deficiencies in cybersecurity controls violated internal accounting controls requirements under Section 13(b)(2)(B) of the Securities Exchange Act of 1934. The ruling underscores the limitations of the SEC's authority to mandate cybersecurity controls, emphasizing that internal accounting controls are intended to ensure the accuracy of financial information, not to address cybersecurity issues. Although this ruling rejects the use of internal accounting controls

as a cyber enforcement tool, the SEC continues to have other available approaches, including charging violations of the disclosure controls and procedures requirements as in the *Flagstar* case.

Cybersecurity Outlook at the SEC

Paul Atkins, the new administration's SEC chair nominee, is expected to transition into his position pending Senate confirmation and as a result, the extent to which cybersecurity will remain a key area of the SEC's focus is uncertain. Notably, sitting commissioners Mark Uyeda and Hester Peirce have openly criticized the SEC's recent approach to cybersecurity enforcement and voted against the disclosure rules adopted in 2023. In a joint dissenting statement in October 2024, in connection with settlements with four technology companies—each of which was a downstream victim of the 2020 SUNBURST cyber-attack—both commissioners expressed concerns about the agency's aggressive stance and questioned the effectiveness of disclosures under Item 1.05. Further complicating the landscape, the SEC faces competing priorities, most notably cryptocurrency regulation, which may divert focus and resources away from cybersecurity initiatives.

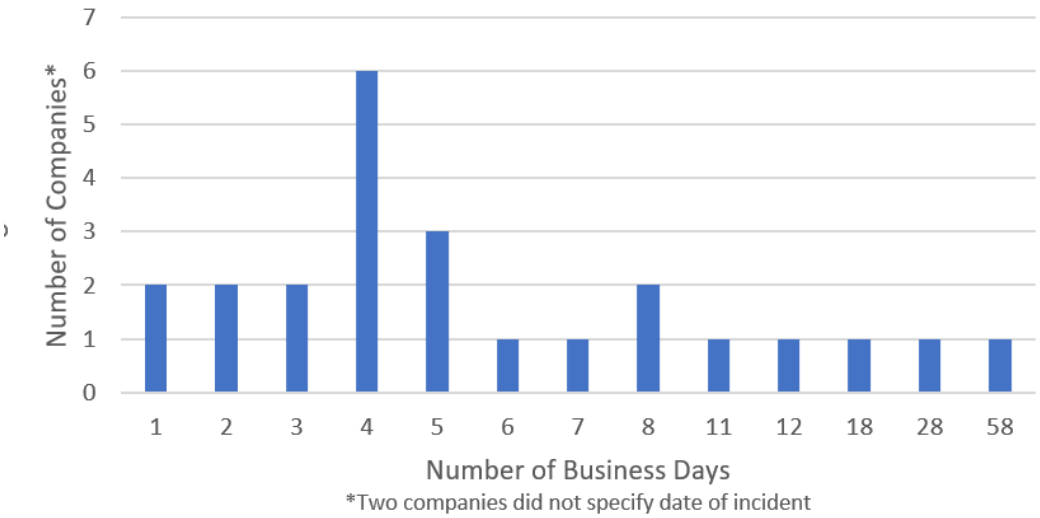
Key Statistics from a Year of Cybersecurity Incident Reporting on Form 8-K

Timing of Cyber Form 8-Ks

Item 1.05 requires a registrant to file a Form 8-K disclosing specified information about a cybersecurity incident within four business days of determining that the cybersecurity incident is material. This four-business-day deadline runs from the materiality determination rather than the occurrence or detection of the incident, and the SEC has acknowledged that "[i]n the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered." The average length of

time between detection of an incident and disclosure of the incident under Item 1.05 has been 7.88 business days, the median length of time has been 4.5 business days, and nearly half have filed within four business days of detecting the cybersecurity incident. While all disclosure decisions will necessarily be driven by the facts and circumstances surrounding the incident, including regulatory or contractual notification requirements, companies should take care not to rush disclosure. In adopting Item 1.05, the SEC acknowledged that registrants will need to "develop information after discovery until it is sufficient to facilitate a materiality analysis." Companies therefore have the opportunity to undertake reasonable investigations and informed and deliberative materiality analysis, provided they do not "unreasonabl[y] delay" the required determination. In most instances, we believe companies are well-advised to exercise caution before rushing to disclose early in the course of an incident investigation. Still, in certain cases, the incident will have public ramifications that may merit very quick disclosure.

Business Days Since Detection



Substance of Cyber Forms 8-K

65%

OF REGISTRANTS HAVE DISCLOSED AN OPERATIONAL DISRUPTION

More than half of the companies that have reported a cybersecurity incident under Item 1.05 disclosed, either in their initial Form 8-K or an amendment, an operational disruption related to the cybersecurity incident. In contrast to financial or more qualitative (*e.g.*, reputational) impacts, operational disruptions may be

more readily identifiable in the early stages of an incident, when disclosure decisions are typically being made. Notably, the operational disruptions disclosed by 14 companies were caused, at least in part, by efforts to remediate or mitigate the incidents.

77%

OF REGISTRANTS HAVE REPORTED ACCESS TO, OR LOSS OF, DATA

Twenty companies have disclosed a cybersecurity incident under Item 1.05 that resulted in access to or exfiltration of data, such as client or customer data, or information contained within corporate email accounts. Six of these companies disclosed the nature of the exfiltrated data or the information targeted by the relevant threat actor in the initial Form 8-K, while nine disclosed this information in a subsequent Form 8-K amendment.

23%

OF REGISTRANTS HAVE IDENTIFIED A THREAT ACTOR

Six of the cybersecurity incidents reported on Item 1.05 included identification—by name or nature—of the suspected threat actor. Three companies initially disclosed the potential involvement of a nation-state actor, two of which identified Midnight Blizzard/Cozy Bear. However, one company that initially attributed the incident to a nation-state later amended its Form 8-K to disclose that the threat actor was in fact a cybercrime group. Another company disclosed the nature of the suspected threat actor, a cybercrime group, on a Form 8-K amendment. Two companies disclosed the potential involvement of cybercrime groups, without identifying the suspected threat actors by name.

In addition, while one company disclosed the possibility of paying a ransom in a cautionary statement in its Item 1.05 disclosure, no companies disclosed payment of a ransom in connection with a cybersecurity incident.

Form 8-K Amendments

50%

OF REGISTRANTS HAVE FILED AN AMENDMENT

To the extent any required information is not determined or is unavailable at the time of filing a Form 8-K under Item 1.05, a company is required to file a Form 8-K amendment containing such information within four business days after the information is determined or becomes available.

Thirteen companies have filed Form 8-K amendments relating to material cybersecurity incidents. These amendments have disclosed remediation of the relevant cybersecurity incident, details regarding the impact of the incident (including the material or immaterial nature of certain impacts), further actions taken by the threat actor and details regarding the nature of the incident.

Item 8.01 Forms 8-K and Subsequent Item 1.05 Forms 8-K

Three companies initially disclosed cybersecurity incidents on Item 8.01 before subsequently filing on Item 1.05, all of which followed the Statement. Two of these companies disclosed on Item 8.01 that they had not yet determined whether the incident was reasonably likely to materially impact financial condition or results of operations. In the subsequent Item 1.05 disclosure, one of these companies disclosed its determination that the cybersecurity incident was reasonably likely to have a material impact on its results of operations, and, in a subsequent amendment, that the incident had a material impact on its business and its results of operations. The second company disclosed that although the cybersecurity incident had a material impact on business operations, the incident did not have a material impact on overall financial condition or results of operations. On the other hand, the third company did not include disclosure as to a determination of materiality in its Item 8.01 disclosure, and, in its Item 1.05 disclosure, stated that the incident did not have, or was not reasonably likely to have, a material impact on the company's financial condition or results of operations. This company's Item 1.05 disclosure also stated that the company remained "subject to various risks due to the incident, including the adequacy of processes during the period of disruption, diversion of management's attention, potential litigation, changes in customer behavior, and regulatory scrutiny," suggesting that the Form 8-K under Item 1.05 may have been filed due to a potential material impact in any one of these areas. In a subsequent Form 10-Q, this company included an additional risk factor specifically addressing certain risks related to cybersecurity threats as well as its reported

cybersecurity incident, but did not include any statement regarding the materiality of the incident.

Conclusion

When the cybersecurity disclosure rules went into effect a year ago, there was uncertainty as to the disclosure burdens and costs that would accompany cybersecurity incident reporting. A year after the rule's enactment, the expectations for disclosing cybersecurity incidents under Item 1.05 of Form 8-K have become clearer. Registrants should disclose only those cybersecurity incidents for which they have identified reasonably likely material impacts under Item 1.05. If a cybersecurity incident will materially impact a registrant's business—financially, reputationally or otherwise—the company must file a Form 8-K under Item 1.05 within four business days of making the materiality determination and must include a description of all reasonably likely material impacts. Companies should maintain open channels of communication between their incident response teams and their disclosure personnel, and should ensure robust disclosure controls and procedures are in place to facilitate the materiality assessment and to facilitate timely and accurate disclosure of any material cybersecurity incident.

We will continue to monitor developments regarding material cybersecurity incidents reported on Form 8-K under Item 1.05 and will provide updates as they become available.

Our Cybersecurity Incident Disclosure Tracker can be found here.

To subscribe to our Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

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

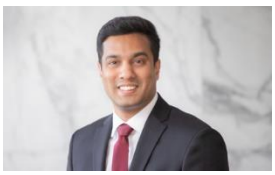
Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

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

Paul M. Rodel
Partner, New York
+1 212 909 6478
pmrodel@debevoise.com

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

Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
amoody@debevoise.com



John Jacob
Associate, New York
+1 212 909 6795
jjacob@debevoise.com

Talia Lorch
Associate, New York
+1 212 909 6707
tnlorch@debevoise.com

Cindy Tu
Law Clerk, New York
+1 212 909 6980
ktu@debevoise.com

This publication is for general information purposes only. It is not intended to provide, nor is it to be used as, a substitute for legal advice. In some jurisdictions it may be considered attorney advertising.