October 25, 2024

A year in review: *The New SEC Cyber Disclosure Rules*

Christopher Porter
CISO, Fannie Mae

Lauren Baraldi
Senior Cyber Counsel, SAP

Evan Roberts
FTI Consulting

Paul Dudek
Latham & Watkins LLP

Tony Kim
Latham & Watkins LLP

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Christopher Porter
SVP and CISO

Fannie Mae

Lauren Baraldi
Senior Legal Counsel, Cybersecurity

SAP

Evan Roberts
Senior Managing Director

FTI Consulting

Paul Dudek
Partner

Latham & Watkins LLP

(former SEC - Chief of the Office of International Corporate Finance)

Tony Kim
Partner

Latham & Watkins LLP

The New Rules

In a Nutshell

Privacy+ Security Forum

SEC Cyber Disclosure Rules

Privacy+ Security Forum

Form 8-K | Item 1.05

- ✓ **Disclose** any "cybersecurity incident" determined "without unreasonable delay" to be **material** and describe material aspects of incident's:
  - nature, scope and timing; and
  - impact or reasonably likely impact (e.g., financial/operational results)
- ✓ **File** Item 1.05 Form 8-K **within four (4) business days** of determining an incident is material, absent national security/safety/FCC exception
- ✓ **Amend** prior Item 1.05 Form 8-K to disclose information that was not determined or unavailable at time of initial Form 8-K filing

Form 10-K

Item 106(b) | *Risk management and strategy*

- ✓ **Describe** (i) **processes**, if any, for the assessment, identification, and management of material cyber risks and (ii) whether any cyber risks have materially affected or are reasonably likely to **affect business strategy, result of operation, or financial condition**

Item 106(c) | *Governance*

- ✓ **Describe** (i) **board's oversight** (e.g., committees, processes) of cyber risks and (ii) **management's role** in assessing and managing material cyber risks (e.g., positions/committees; expertise; processes for preventing, monitoring, detecting, mitigating incidents; reporting to the board)

Compliance Deadlines

December 18, 2023
(June 15, 2024 for smaller companies)

Annual Reports starting for Fiscal Years ending on or after December 15, 2023

What's Happened in the Market under the new rules?

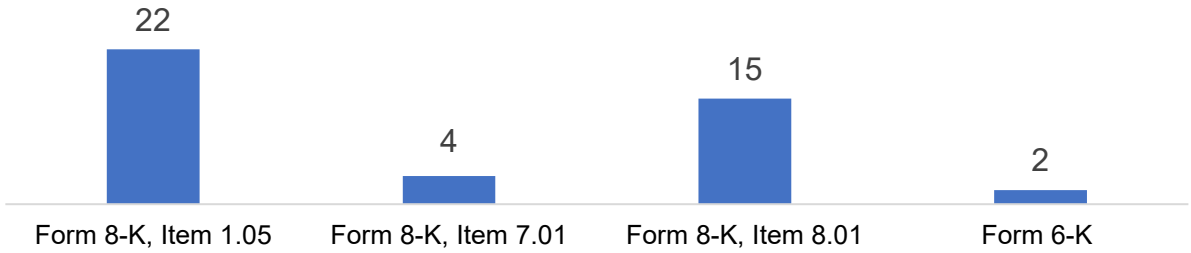
Privacy+ Security Forum

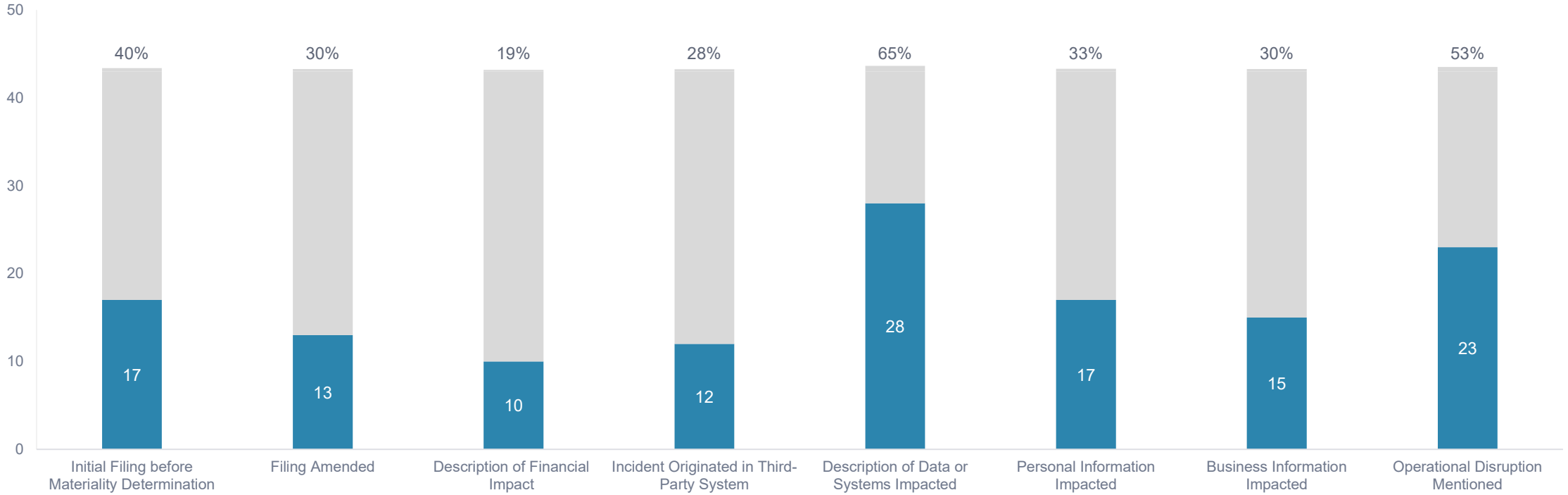
Cyber Disclosure Trends

- Item 1.05 filings in early 2024 often disclosed:
  - There was no material impact on the company's business or operations; and
  - The incident was not expected to have (in the future) a material impact on the company's financial condition or results of operations; or
  - The company had not yet determined if a material impact was reasonably likely
- Typically, relatively limited information was provided in initial filings with a focus on high-level response/containment steps and identifying third parties engaged to assist
  - Subsequent amendments provided additional detail and updates on incident resolution and investigation efforts
- After SEC guidance issued in May 21, 2024 cautioning against "voluntary" use of Item 1.05, there was an increase in Item 8.01 and 7.01 Form 8-Ks disclosing cyber incidents
- U.S. Attorney General granted at least one *delayed Item* 1.05 Form 8-K disclosure

Cyber Disclosure Trends

Select cohort examined:
43 cyber disclosures, Form 8-K
(Dec. 18, 2023 thru Sept 2024)





What's Up with These Form 8-Ks?

Privacy+ Security Forum

Implementing the New Rules

Privacy+ Security Forum

“Materiality”

- Quantitative (and) (versus) (or) Qualitative?
- How do you *measure* materiality?
- What is “reputational harm”?
- Is there any distinction between a “material **incident**” and a “material **impact**”? Can you have the former but not the latter?

No, but seriously, what is a “material” incident that triggers Item 1.05?

No, but seriously . . .

Privacy+ Security Forum

Audience Poll:

Is a single laptop or single email account compromise potentially material?

No, but seriously . . .

Privacy+ Security Forum

Audience Poll:

Is ransomware automatically material and requires an Item 1.05 Form 8-K?

No, but seriously . . .

Privacy+ Security Forum

Audience Poll:

What if your major (critical) service provider files a Form 8-K, is that material for you too?

No, but seriously . . .

Privacy+ Security Forum

Audience Poll:

What if your major (critical) service provider does NOT file a Form 8-K, is that a pass for you too?

SEC Guidance (May 21, 2024)

STATEMENT

Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents

Erik Gerding, Director, Division of Corporation Finance

- If company chooses to disclose a cyber incident for which it not made a materiality determination, or determined it was not material, then SEC "encourages" use of a different item Form 8-K (for example, Item 8.01).
- "It could be confusing for investors if companies disclose either immaterial cybersecurity incidents or incidents for which a materiality determination has not yet been made under Item 1.05."
- In assessing materiality, "companies should assess all relevant factors," not only impact on "financial condition and results of operation," but "qualitative factors alongside quantitative factors" such as "reputation, customer or vendor relationships, or competitiveness." Companies also should consider "the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal Governmental authorities and non-U.S. authorities."
- "There also may be cases in which a cybersecurity incident is so significant that a company determines it to be material even though the company has not yet determined its impact (or reasonably likely impact)."

Stakeholder Experiences to date

Privacy+ Security Forum

Confusion? Frustration? Fear? CYA?

Privacy+ Security Forum

“Materiality” Determinations

- How does Management and the Board feel about these new rules?
- What about CISOs?
- What about In-House Counsel?
- What about “Disclosure Decision-Makers”?

What process changes have occurred to account for the new regime?

12 FAQs from the C-Suite and Boardroom

Privacy+ Security Forum

1	Is “cybersecurity incident” the same as “data breach”?	No; “cybersecurity incident” is MUCH broader than “data breach” (e.g., cybersecurity incidents require no impact to data at all and could be wholly operational in nature)
2	Are incidents at third-party service providers out-of-scope?	No; third-party incidents can materially impact registrants, and the new rules encompass information systems “used” by registrants
3	When does the 4-business-day clock for Item 1.05 start?	When the registrant determines that the incident is “material”
4	How quickly must we assess materiality?	“Without unreasonable delay” after discovery
5	What does “material” mean?	Reasonable investor would care based on both quantitative and qualitative factors; see next slide
6	Are there exceptions to the 4-business-day filing deadline?	No -- except for extremely narrow exceptions for national security and public safety, and for certain CPNI/FCC breaches
7	Are accidental incidents considered “unauthorized”?	Yes; malicious activity is not required
8	Should we err in favor reporting under Item 1.05 as a C.Y.A. if we think the incident is not material, but its close?	Item 1.05 irrevocably concedes materiality; many factors to consider and Items 7.01 and 8.01 may offer more flexibility for marginal incidents
9	Why are companies filing 8-Ks for “non-material” issues?	Materiality includes qualitative factors, even if operations/results are fine; also, some companies have inadvisably used Item 1.05 despite immateriality
10	Is “ransomware” an automatic Item 1.05, Form 8-K?	Nothing is automatic; the test is material impact, not incident type, but ransomware is often material
11	If an incident triggers notifications under GDPR or state breach notice laws, does that automatically require a Form 8-K too?	No. Notifications under GDPR, HIPAA, etc. address impacts to certain data types, whereas the SEC is focused on materiality to investors
12	Has the SEC Staff issued a comment letter on Item 1.05 disclosure?	Yes; and emphasized that “all material impacts” includes “potential reputational harm,” not only operations/results, and required 8-K/A amendment for later determinations of materiality

Don’t forget about new Form 10-K rules!

Privacy+ Security Forum

Key challenges

- Distinguishing aspirational goals versus factual processes
- Is “less is more” the way to go?
- Wordsmithing and scrutinizing word choice
- Assembling back-up for each and every disclosure made in new Item 1C
- Taming your marketing teams and ESG report!

What process changes have occurred to account for the new regime?

Discussion

-and-

Thank You!

Privacy+ Security Forum