PAUL
HASTINGS

SEC Cybersecurity Incident Disclosure Report

December 2024

Executive Summary

Paul Hastings' SEC Cybersecurity Incident Disclosure Report provides directors, officers, executives, security leaders and in-house counsel with quantifiable evidence relevant to disclosure decision making. This report analyzed 75 disclosures issued by 48 public companies that disclosed cybersecurity incidents between December 18, 2023 and October 31, 2024.

Key Takeaways:

- **Since the SEC rules became effective, there has been a 60% increase in the number of cyber incidents disclosed by public companies.**
- **Fewer than 10% of the disclosed incidents include a description of the material impact.**
- **78% of disclosures were made within eight days of discovery of the incident, with 42% of companies providing an update by issuing an updated Form 8-K after the initial disclosure.**
- **Third-party breaches had the widest ranging impact for public companies, with one in four breaches stemming from a third-party incident.**
- **Threat actors used the SEC rules as an extortion tactic, with threat actors themselves submitting whistleblower reports to the SEC regarding failure to disclose and then publishing them online.**

Introduction

The Securities Exchange Commission (SEC) approved new rules around Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure in July 2023. The rules created a new series of requirements for public companies to disclose material Cybersecurity Incidents beginning on December 18, 2023.

The rules specifically require that public companies comply with the following:

- Public companies must disclose all material Cybersecurity Incidents within four business days of determining that the incidents are material. Companies must assess materiality of a Cybersecurity Incident without unreasonable delay following discovery.
- The disclosure should include the nature, scope and timing of the incident and the impact or reasonably likely impact of the incident on the company, its financial condition and its results of operations.
- The rules do not require companies to disclose specific or technical information about their planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in detail that would impede remediation.
- If new information becomes available after the initial filing of the Form 8-K and such information impacts the materiality of the cybersecurity incident, the company is required to amend its Form 8-K within four business days of that information becoming available.
- A series of *related* Cybersecurity Incidents may require an 8-K filing even if they are all not material. The SEC removed the requirement to report an aggregation of "immaterial incidents" on Forms 10-Q and 10-K.

The rules have presented new challenges for public companies over the past year in (1) determining which Cybersecurity Incidents are material, (2) when and how they need to be disclosed to the SEC on a Form 8-K and (3) what information should be reported. Paul Hastings analyzed these disclosures including:

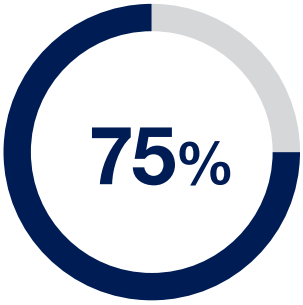
- What information public companies disclosed about Cybersecurity Incidents.
- How public companies disclosed these Cybersecurity Incidents to the SEC.
- How public companies should think further about compliance with the rules moving into 2025.

The year of disclosures led to significant insights related to types of Cybersecurity Incidents disclosed, timing of the breach, content of the breach and many others.

Headliners

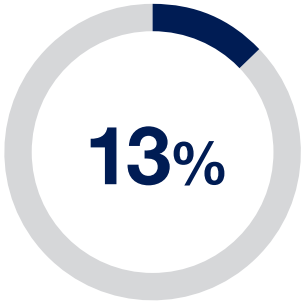
1 in 4 incidents disclosed were third-party vendor incidents

The SEC recently announced enforcement settlements with four companies for allegedly making materially misleading disclosures related to the SolarWinds incident. All four companies were SolarWinds customers that were impacted when their vendor suffered an attack at the hands of a sophisticated nation-state actor. Two of the four companies publicly disclosed the cybersecurity incidents in a Form 8-K. However, the SEC alleged that the disclosures were materially misleading, in part, because they did not disclose all material facts known to the company at the time (e.g., did not disclose the name of the threat actor, nature of information taken or number of accounts accessed). The other two companies did not publicly disclose the cybersecurity incidents, but the SEC claimed that their 10-Q and 10-K risk disclosures were misleading in light of the SolarWinds' impact on the company.



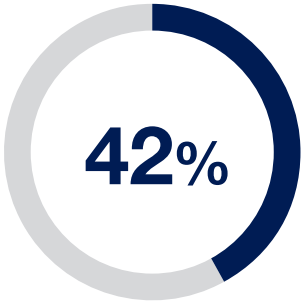
75% of disclosed Cybersecurity Incidents included a reference that law enforcement was notified

The SEC permits a delay in reporting material Cybersecurity Incidents if the disclosure would present a substantial risk to national security or public safety, in which case the attorney general must notify the SEC in writing of such risks. Mere notification to law enforcement does not by itself justify a delayed disclosure.



13% of disclosed Cybersecurity Incidents provided more details by including a press release as an exhibit or referencing a blog in at least one of their disclosures

Companies often wrestle with the level of detail to include in the Form 8-K. Some companies have used Exhibit 99.1 to include additional details such as a press release or a blog reference. Exhibit 99.1 is broadly considered a catch-all category in which to provide additional documents and ensure transparency to investors.

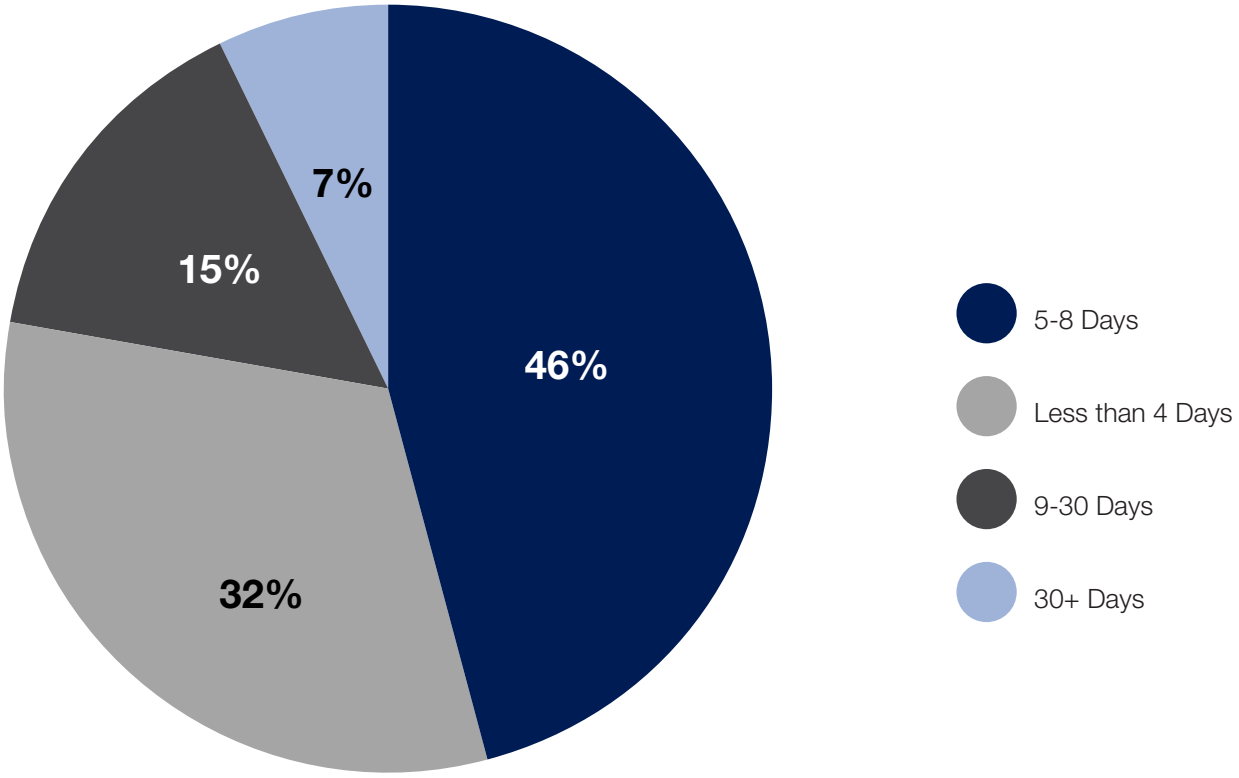


42% of companies filed more than one disclosure for the same Cybersecurity Incident, typically by issuing an updated Form 8-K after the initial disclosure

When filing under Item 1.05, the SEC rules impose an obligation on companies to update within four business days of learning information that impacts the materiality of the incident. Companies provided updates on a wide range of issues, including quantifiable loss, impact to customer personal data, notification to individuals and regulators and so forth.

Timing of Disclosure

Time Between Awareness and Filing



Although the SEC expressly noted that the deadline to disclose is *not* four business days after the incident occurred or is discovered, most disclosures happened quickly, with 32% filing within four days from discovery and 78% within eight days from discovery. The SEC requires that companies make a materiality determination "without unreasonable delay" but notes that "a materiality determination necessitates an informed and deliberative process." Companies should continue to evaluate disclosure controls and engage in tabletop exercises to practice the decision-making required to makes such materiality decisions in the event of a cyber incident.

Materiality

The SEC rules set materiality as the threshold requiring disclosure, noting that information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the 'total mix' of information made available." In determining materiality, the SEC instructed public companies to evaluate both quantitative and qualitative factors, considering: immediate fallout and any longer-term effects on its operations; customer relationships; financial impact; reputational or brand perception; and the potential for litigation or regulatory action.

Fewer than 10% of companies specified the material impact in their disclosures.

What was disclosed as material?

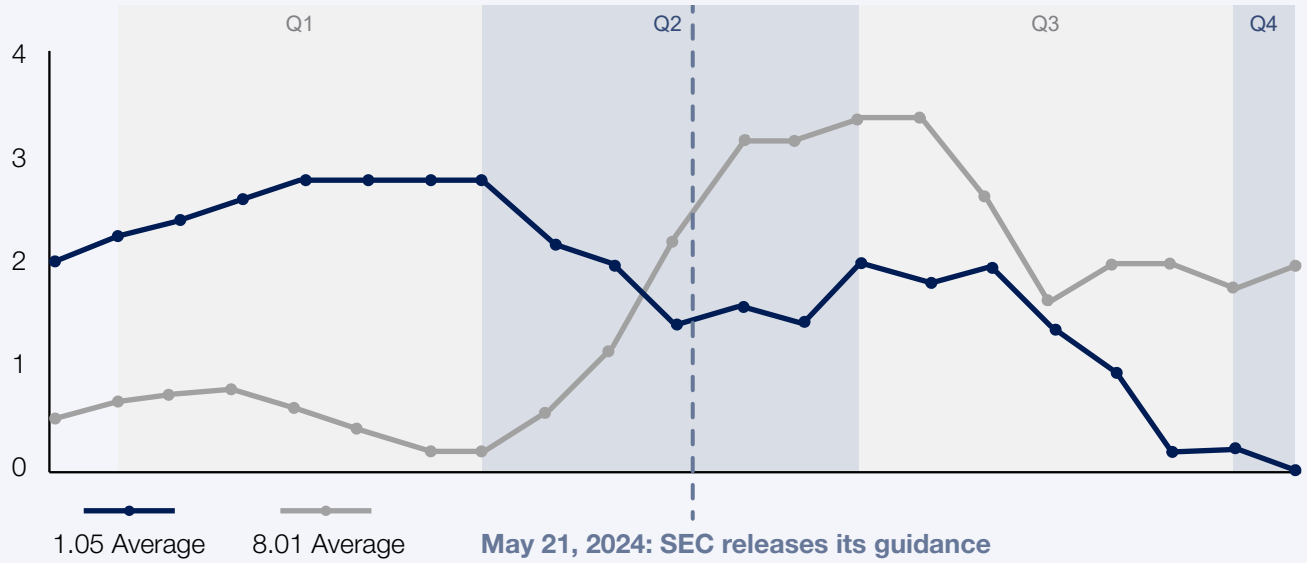
Company and 8K filings	What Was Materially Impacted?	Adjusted Earnings Per Share?	Losses Quantified in 10-Q/10-K?
Bassett Furniture Industries, Inc.	Business operations until recovery efforts are completed	No	Yes
Crimson Wine Group, Ltd.	Business operations as of the date of the 8K	No	No
Sonic Automotive, Inc.	Quarterly results of operation for the second quarter	Yes	Yes
Key Tronic Corp	Financial condition and results of operations for the fourth quarter	No	Yes
First American Financial Corp.	Results of operations for the fourth quarter	Yes	Yes

As public companies began disclosing incidents, the SEC found that companies were too often disclosing immaterial incidents under Item 1.05 and issued clarifying guidance. The SEC's Division of Corporation Finance (Corp Fin) released a statement on May 21, 2024, reminding companies that they should only disclose *material* incidents on Form 8-K under Item 1.05, adding that incidents that are initially not material can be filed under Item 8.01. On June 24, 2024, Corp Fin released a series of "Compliance and Disclosure Interpretations" that provided further guidance on how to determine whether incidents are material:

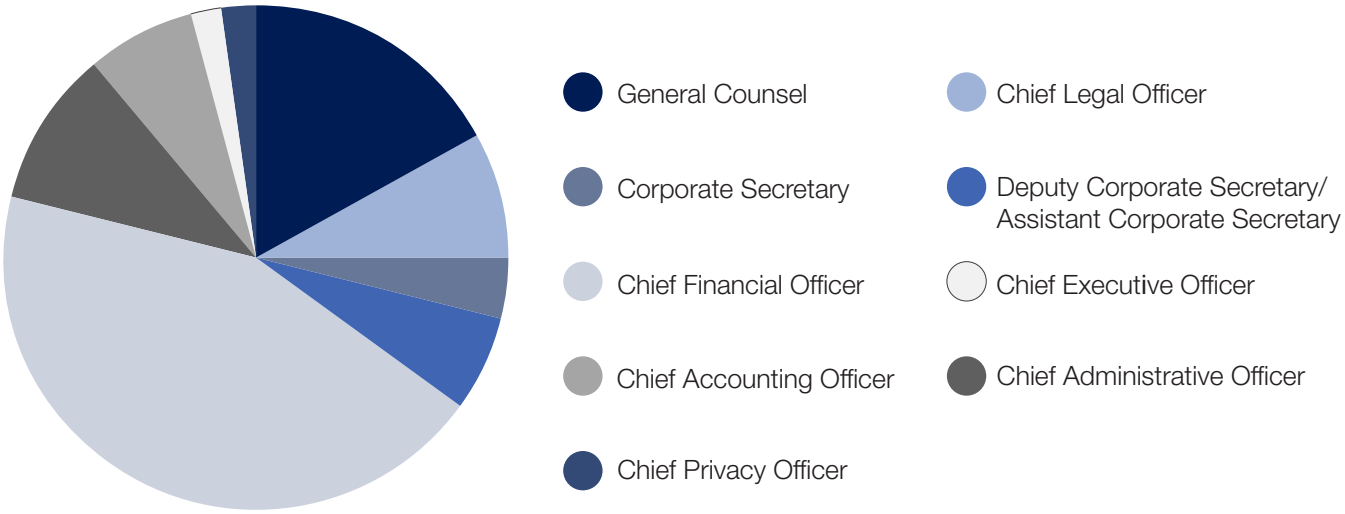
- If the incident ends before a materiality assessment is complete, the company must still assess the materiality of the incident.
- If a company determines a ransomware attack is material and makes a payment that causes the attack to end before reporting, the company is not relieved of the requirement to disclose the incident.
- The need to make a ransomware payment or the amount of such payment should not be the sole factors in determining materiality.
- Having a cyber insurance policy that reimburses companies for costs related to an incident does not preclude companies from having to conduct a materiality assessment and potentially disclosing the incident.
- A company experiencing a series of incidents that are individually considered immaterial, should determine whether in the aggregate, they would be material.

Following the SEC's guidance in May and June 2024, companies filed at the same rate, but many switched from filing under Item 1.05 to filing under Item 8.01.

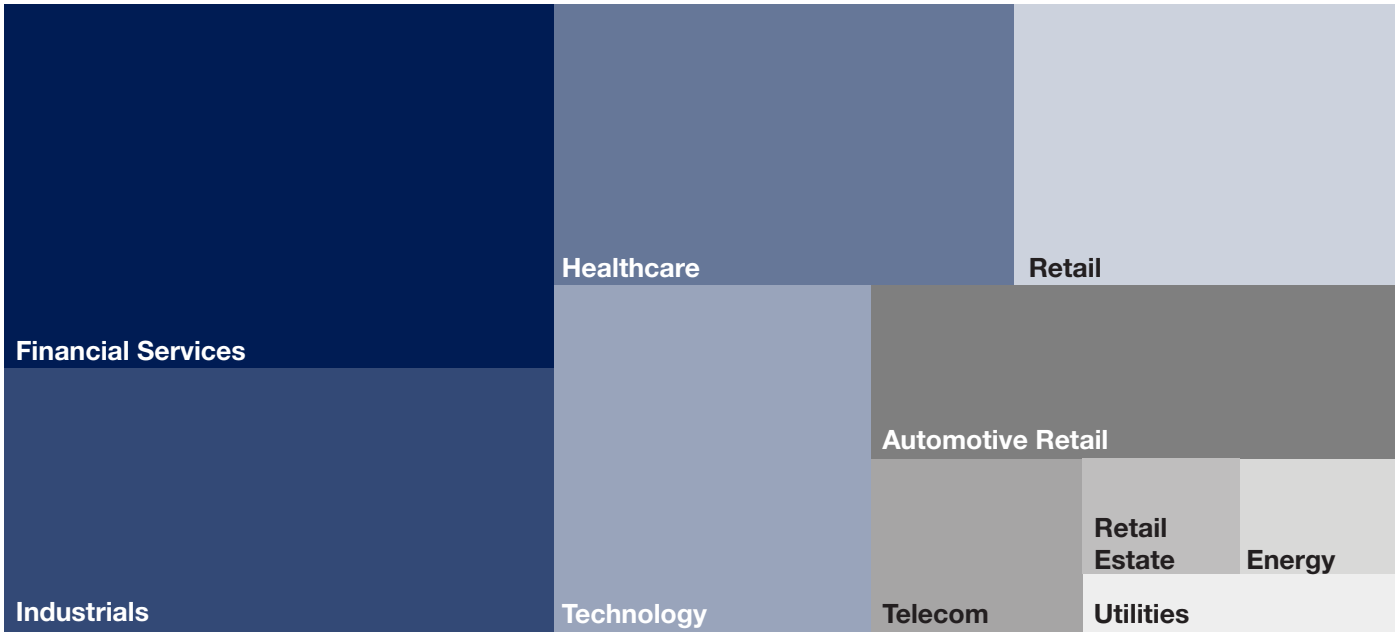
Changing Type of Disclosures Over Time

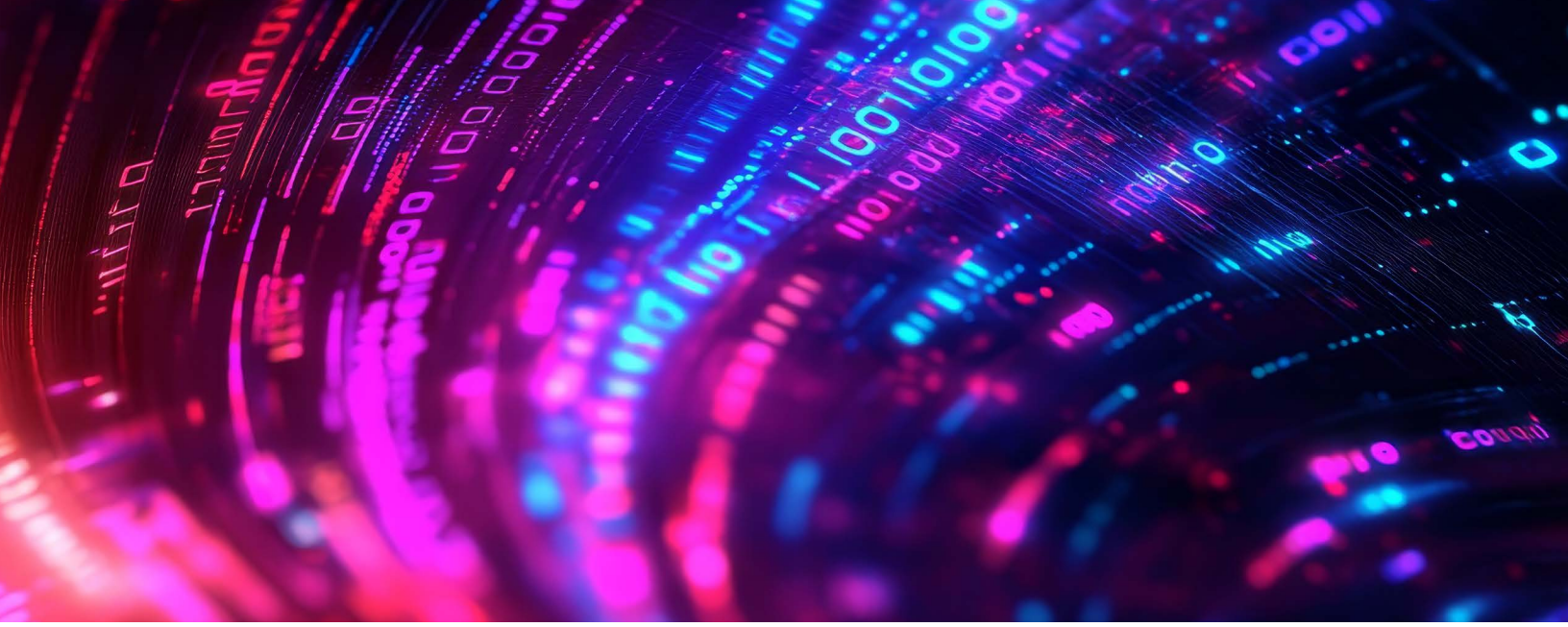


Who Files the Form 8-K



Which Industries Were Affected





An Unexpected Whistleblower: The Threat Actor

In an aggressive move to pressure victims into paying ransoms, some threat actors have filed whistleblower reports with the SEC, claiming that companies have failed to report active incidents on Form 8-K. The threat actor then makes its "whistleblower" report public, attempting to publicly shame victims and encourage payment. While such tactics have failed each time, they have generated significant media attention, with over 40 news articles published in publications such as *The Wall Street Journal*, *Bloomberg*, *Security Week* and others.

The Wall Street Journal
A Ransomware Gang Wanted Its Victim to Pay Up. So It Went to the SEC.

Law.com
In What Could Be a Trend, Ransomware Operation Files SEC Complaint Against Victim for Failing to Timely Disclose Cyberattack

Security Week
Ransomware Group Files SEC Complaint Over Victim's Failure to Disclose Data Breach

Recommendations

Public companies should continue to evaluate disclosure controls and test internal processes to ensure swift and fulsome disclosure of material Cybersecurity Incidents. With SEC enforcement of cybersecurity matters on the rise, it is essential for companies to prepare. The Paul Hastings Data Privacy and Cybersecurity team regularly advises on compliance with cybersecurity regulations. If you have any questions concerning how these requirements may affect your organization, please do not hesitate to contact a member of the Paul Hastings team.

Authors

Sherrese Smith
Global Managing Partner

Sherrese Smith is the Managing Partner of Paul Hastings. She is known as one of the country's preeminent Data Privacy and Cybersecurity and Media and Technology attorneys and she is recognized throughout the legal, media, communications and technology industries for her leadership, business acumen and dedication to clients. Her work includes data privacy, cybersecurity and breach response issues, crisis response, regulatory investigations and enforcement proceedings, as well as counseling on global privacy and cybersecurity matters.

Michelle Reed
Co-Chair
Data Privacy and Cybersecurity

Michelle Reed is Co-Chair of the Data Privacy and Cybersecurity group and is a partner in the Litigation Department at Paul Hastings. She is based in the firm's Dallas office. Recognized by Chambers USA and Chambers Global, Michelle has two decades of experience advising companies, boards and executives on navigating the evolving risks in privacy and cybersecurity regulation, enforcement and class action litigation.

Aaron Charfoos
Co-Chair
Data Privacy and Cybersecurity

Aaron Charfoos is Chair of the Chicago Litigation Department and Co-Chair of the Data Privacy and Cybersecurity group. He is an accomplished cybersecurity, privacy, class action and data protection trial lawyer. Aaron has litigated a variety of privacy and cybersecurity cases including data breach class actions, Video Privacy Protection Act (VPPA), Illinois Biometric Information Privacy Act (BIPA), California Invasion of Privacy Act (CIPA) and other pixel and third-party tracking technology cases. Aaron also defends clients in regulatory investigations brought by various U.S. and international regulatory bodies.

Dave Coogan
Associate

Dave Coogan advises public and private clients in data privacy and cybersecurity litigation and investigatory matters. As a former military prosecutor who has tried cases before a jury, he has litigation experience that provides clients with an important perspective during internal investigations and in responding to privacy and cybersecurity regulators.

Jeremy Berkowitz
Senior Director

Jeremy Berkowitz is a Senior Director in the Paul Hastings Privacy and Cybersecurity Solutions Group. He has both a thorough understanding of global privacy and cybersecurity laws/regulations, and extensive experience helping organizations understand the gaps in their programs. He has worked with clients for almost 15 years on pursuing the best strategies to enhance their privacy and cyber risk footprints.

Additional Contributors

Hannah Edmonds, Associate

Kimia Favagehi, Associate

Rachel Kurzweil, Of Counsel

Marisa Polowitz, Associate

Jennifer Ash, Director, Research

Jason Dirkx, Director, Innovation and Technology Solutions

Scott Kaiser, Knowledge and Innovation Attorney

Heather O'Dea, Legal Research Analyst

Andrew Wood, Legal Technologist