SEC Enforcement Case Summary
Public Company Charged with Misleading Investors Regarding Cyber Incident

On January 13, 2025, the Securities and Exchange Commission (***SEC***) charged Ashford Inc., a former public company, with providing misleading information in public filings regarding a cyber incident. Ashford is an alternative asset management company with a portfolio of strategic operating businesses that provide global asset management, investment management, and related services to the real estate and hospitality sectors. According to the SEC's complaint, Ashford learned in September 2023 that it had been subjected to a cybersecurity attack and ransomware demand by a foreign-based threat actor. As part of the attack the threat actor gained access to Ashford's servers and exfiltrated more than 12 terabytes of data which was stored on Ashford's internal computer systems. The data contained, among other things, sensitive hotel guest information including but not limited to sensitive personally identifiable information (***PII***) and financial information for some of Ashford's customers.

Ashford first disclosed the cyber incident in its report for the quarter ending September 30, 2023, filed with the SEC on November 13, 2023 (***Q3 10-Q***). Ashford stated in its Q3 10-Q that the September 2023 cyber incident resulted in "potential exposure of certain employee personal information." Ashford went on to state, "[w]e have completed an investigation and have identified certain employee information that may have been exposed, but we have not identified that any customer information was exposed." Ashford made similar misleading disclosures in two additional quarterly reports, along with Ashford's annual report filed with the SEC for the period ended December 31, 2023. However, the SEC noted that Ashford knew or should have known that the exfiltrated data contained sensitive personally identifiable information and financial information related to guests.

Ashford first learned of the cyber incident on September 20, 2023 when the threat actor locked several critical servers and demanded a ransom from Ashford to provide the decryption key, which they requested to be paid in Bitcoin. The threat actor provided Ashford with a list of files it exfiltrated and notified Ashford that guest incident reports were included among the exfiltrated documents. According to the complaint, Ashford had established an incident response plan (***IRP***) that outlined a process to determine whether customer information and/or financial data was exfiltrated in a security incident. However, the company did not follow the IRP or effectively review the file information for PII. The SEC alleged that had Ashford done so it would have known that PII was compromised.

Ashford agreed to settle the SEC's charges, consenting to an injunction and an order to pay a civil penalty of $115,231, which takes into account Ashford's assistance to the SEC staff in its investigation. This case reinforces the importance of adopting and actively following a robust IRP in the event of a potential security breach. This will be paramount upon the compliance date for the recent amendment to Regulation S-P that will impact large registered investment advisers (with more than $1.5B in assets) in December 2025 and those with less than $1.5B in assets in June 2026. Moreover, it is critical that disclosures to clients and investors regarding security breaches are accurate and to not underplay the impact of such events.

See Summary – https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26215