IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **v.** **ASHFORD INC.,** **Defendant.**	**Civil Action No. 3:25-cv-00082** **Jury Trial Demanded**

COMPLAINT

Plaintiff United States Securities and Exchange Commission ("SEC") files its Complaint against Ashford Inc. ("Ashford" or "Defendant") and alleges as follows:

SUMMARY

1. Ashford, a company that provides products and services to the real estate and hospitality industries, made false and misleading disclosures in periodic reports filed with the SEC regarding a cybersecurity incident that Ashford experienced.

2. In September 2023, Ashford learned 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 approximately 12 terabytes of data which was stored on Ashford's internal computer systems, and informed Ashford, among other things, that they had obtained sensitive hotel customer information ("September 2023 Cyber Incident").

3. Ashford, a publicly traded company at the relevant time, was required to file periodic reports with the SEC. The federal securities laws further require that those reports contain, in addition to disclosures expressly required by statute and rules, such other material

information as is necessary to ensure that the statements made are not, under the circumstances, misleading.

4. Ashford first disclosed the September 2023 Cyber Incident in its report for the quarter ending September 30, 2023, filed with the SEC on November 13, 2023 ("Q3 2023 10-Q"). Ashford stated in its Q3 2023 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*." (Emphasis added). Ashford made similar disclosures in two additional Forms 10-Q, along with Ashford's most recent annual report filed on Form 10-K on March 27, 2024, for the period ending December 31, 2023 ("2023 10-K").

5. Ashford, however, knew or should have known that, contrary to its public disclosures, customer information was exposed, because, as Ashford knew or should have known, the files exfiltrated in the September 2023 Cyber Incident did contain customer information, including but not limited to sensitive personally identifiable information ("PII") and financial information for some of Ashford's customers.

VIOLATIONS

6. After Ashford filed its Form 10-Q for the period ending March 31, 2024, on May 13, 2024 ("Q1 2024 10-Q"), in which the company made substantially the same false and misleading disclosure regarding the September 2023 Cyber Incident, Ashford awarded stock and deferred stock grants to its directors. By including in its Q1 2024 10-Q the materially misleading disclosure that, after completing its investigation regarding the September 2023 Cyber Incident, it had not identified any exposed customer information, which Ashford knew or should have

known was false and misleading, Ashford violated Section 17(a)(3) of the Securities Act of 1933 ("Securities Act") [15 U.S.C. § 77q(a)(3)].

7. In addition, when Ashford filed its Q3 2023 10-Q, Q1 2024 10-Q, 2023 10-K, as well as its Form 10-Q for the period ending June 30, 2024, on August 13, 2024 ("Q2 2024 10-Q"), each of which contained materially false and misleading disclosures concerning the September 2023 Cyber Incident, Ashford violated Section 13(a) of the Securities Exchange Act of 1934 (the "Exchange Act") [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, and 13a-13 [17 C.F.R. §§ 240.12b-20, 240.13a-1, and 240.13a-13] thereunder.

8. Unless Defendant is restrained and enjoined, it will engage in the acts, practices, transactions, and courses of business set forth in this Complaint or in acts, practices, transactions, and courses of business of similar type and object.

NATURE OF THE PROCEEDING AND RELIEF SOUGHT

9. The SEC brings this action pursuant to the authority conferred upon it by Sections 20(b) and 20(d) of the Securities Act [15 U.S.C. §§ 77t(b) and 77t(d)], and Section 21(d) of the Exchange Act [15 U.S.C. § 78u(d)].

10. The SEC seeks a final judgment: (a) permanently enjoining Defendant from violating the federal securities laws that this Complaint alleges Defendant has violated; (b) ordering Defendant to pay civil money penalties pursuant to Section 20(d) of the Securities Act [15 U.S.C. § 77t(d)] and Section 21(d)(3) of the Exchange Act [15 U.S.C. § 78u(d)(3)]; and (c) ordering any other and further relief, including equitable relief and other relief pursuant to Section 21(d) of the Exchange Act [15 U.S.C. § 78u(d)], the Court may deem just and proper.

JURISDICTION AND VENUE

11. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331, Sections

20 and 22 of the Securities Act [15 U.S.C. §§ 77t and 77v], and Sections 21 and 27 of the Exchange Act [15 U.S.C. §§ 78u and 78aa].

12. Defendant, directly and indirectly, singly or in concert with others, made use of the means or instrumentalities of interstate commerce or of the mails, in connection with the transactions, acts, practices, and courses of business alleged herein.

13. Throughout the relevant period, Ashford was engaged in the offer or sale of securities. Specifically, Ashford offered and sold stock annually to its directors through an equity Incentive Plan for which a Form S-8 was filed with the SEC on November 13, 2014.

14. Venue is proper in this district pursuant to Section 22(a) of the Securities Act [15 U.S.C. § 77v(a)] and Section 27 of the Exchange Act [15 U.S.C. § 78aa] as Defendant's principal place of business is within this district, and certain transactions, acts, practices, and courses of business constituting the violations alleged herein occurred within this district.

DEFENDANT

15. **Ashford** is a Nevada corporation headquartered in Dallas, Texas. Ashford's common stock was registered with the SEC pursuant to Section 12(b) of the Exchange Act and traded on the New York Stock Exchange until July 29, 2024, when it was delisted. On August 8, 2024, Ashford filed a Form 15 with the SEC to terminate registration of its common stock under Section 12(g) of the Exchange Act. The Form 15 became effective on November 6, 2024.

FACTS

I. Background

16. 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.

17. Ashford serves as the advisor to two New York Stock Exchange-listed real estate

investment trusts that together own 83 hotels and have more than $7.5 billion in gross assets.

18. Since December 2022, Ashford maintained an Incident Response Plan ("IRP") to respond to potential cybersecurity attacks.

19. Included within the IRP, the company stated, "[a]n incident is typically either one that compromises functionality (Functional Impact table), or compromises information (Information Impact table). Rare are incidents that combine factors from both tables."

20. The September 2023 Cyber Incident compromised both Ashford's functionality and information.

II. Ashford Discovered a Cyber Incident in September 2023

21. On or about September 20, 2023, Ashford discovered that its internal computer systems were hacked by a foreign-based threat actor.

22. During the incident, the threat actor locked several critical servers, including Ashford's hotel key management servers. As a result, at least 22 hotels within Ashford's network were unable to access certain data for their daily operations.

23. In addition to destabilizing Ashford's computer network, the threat actors exfiltrated approximately 12 terabytes of data stored on Ashford's internal computer systems, which equates to approximately 78 million pages of Ashford data.

24. The threat actor initially demanded a ransom from Ashford to provide the decryption key, which they requested to be paid in Bitcoin. As part of its demand, 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.

25. The file names in the list suggested that the files contained sensitive customer information. For example, hundreds of file names contained titles such as "guest incident report" and "guest folio" with a corresponding customer name and/or date of their stay.

26. Certain Ashford employees whose departments maintained files on the compromised servers were contacted to determine whether the department kept PII on the compromised servers and, if so, whether it related to a customer or employee. Ashford employees who were contacted were not part of the order of notification process listed in Ashford's IRP, nor did they review the file trees for the compromised data.

27. Had they reviewed the file trees for the compromised data, they would have seen customer information or would have been alerted to the possibility of customer information within various documents.

28. Ashford's response was inconsistent with Ashford's IRP, which it established to determine whether customer information and/or financial data was exfiltrated by the threat actor.

29. Some of the exfiltrated files did contain information about customers, including state identification card images, bank account numbers, last four digits of credit card numbers, incident reports, addresses, phone numbers, vehicle descriptions and license plate numbers, folios, and dates of stay.

30. For example, one file contained the sensitive PII of a customer, including a photocopy of the customer's driver's license which identified the name, address, and date of birth for the customer.

31. Another document provided sensitive financial information of a customer, including a copy of the check Ashford received for payment, which identified the name, routing number, and bank account for the customer.

32. As such, Ashford knew or should have known it was likely that customer information was contained within the 12 terabytes of data exfiltrated by the threat actor.

33. On September 25, 2023, Ashford obtained the encryption key and received representations by the threat actor they would destroy the exfiltrated data.

34. Following Ashford's initial disclosure of the September 2023 Cyber Incident in its Q3 2023 10-Q, and in response to voluntary requests from SEC staff, Ashford provided SEC staff with documents, summaries of events, and analysis regarding the September 2023 Cyber Incident.

III. Ashford Negligently Misled Investors Regarding the September 2023 Cyber Incident.

35. On November 13, 2023, Ashford first publicly disclosed the September 2023 Cyber Incident in its Q3 2023 10-Q:

> During the quarter ended September 30, 2023, we had a cyber incident that resulted in the potential exposure of certain employee personal information. We have completed an investigation and have identified certain employee information may have been exposed, but we have not identified that any customer information was exposed. Systems have been substantially restored with minimal effect on certain hotel operations.

36. Ashford discussed the September 2023 Cyber Incident in at least three additional periodic reports filed with the SEC.

37. In the 2023 10-K, Q1 2024 10-Q, and Q2 2024 10-Q SEC filings, Ashford disclosed in relevant part: "During the quarter ended September 30, 2023, we had a cyber incident that resulted in the potential exposure of certain employee personal information. We 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. All systems have been restored."

38. Ashford knew or should have known that its disclosures concerning the September 2023 Cyber Incident in its Q3 2023 10-Q, 2023 10-K, Q1 2024 10-Q, and Q2 2024 10-Q were false and misleading.

39. For example, Ashford initially disclosed in November 2023 in its Q3 2023 10-Q that it had completed its investigation and had not identified any customer information was exposed. Given the steps the company undertook during its internal investigation of the cyber incident, Ashford knew or should have known that that customer information was exposed.

40. The names of the exfiltrated files contained titles such as "guest incident report and "guest folio" with a corresponding customer name and/or date of their stay, suggesting that sensitive customer information was exposed. In addition, "guest incident reports" were among the data the threat actor explicitly claimed to Ashford that it had exfiltrated.

41. Ashford's disclosures remained misleading when Ashford filed its 2023 10-K, Q1 2024 10-Q, and Q2 2024 10-Q, and had been proven false by documents produced by Ashford to the SEC, including hundreds of instances of customer information having been exfiltrated.

42. Ashford's false and misleading disclosures concerning the September 2023 Cyber Incident were also material.

43. As a service provider to hotels, protecting customer information from unauthorized access is critically important to Ashford's business: as Ashford acknowledged in its 2023 10-K, "protection of business partners, employees and company data is critically important to [it]."

44. The September 2023 Cyber Incident not only exposed customers' highly personal information, including PII such as a customer's date of birth, it also exposed customers' financial information, including credit card issuers, last four digits of credit card numbers, and bank account information.

45. In addition, Ashford's materially false and misleading statements were made "in the offer or sale" of securities because, during the relevant period, Ashford offered and sold

stock to its directors through an equity Incentive Plan for which a Form S-8 was previously filed with the SEC on November 13, 2014. Specifically, Ashford awarded stock to directors as part of the plan during the period after the company's misstatements in the Q1 2024 10-Q.

FIRST CLAIM FOR RELIEF
Violation of Section 17(a)(3) the Securities Act

46. The SEC repeats, realleges, and incorporates by reference paragraphs 1 through 45, as though fully set forth therein.

47. Ashford, by engaging in the conduct above, singly or in concert with others, in the offer or sale of securities, by the use of means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly, knowingly, recklessly, or negligently engaged in transactions, practices, or courses of business which operated or would operate as a fraud or deceit upon the purchasers of Ashford stock.

48. By reason of the conduct described above, Defendant Ashford violated, and unless enjoined will continue to violate, Section 17(a)(3) of the Securities Act [15 U.S.C. § 77q(a)(3)]. With regard to the violations of Section 17(a)(3) of the Securities Act, Defendant Ashford acted at least negligently.

SECOND CLAIM FOR RELIEF
Violations of Section 13(a) of the Exchange Act
and Exchange Act Rules 12b-20, 13a-1, and 13a-13 Thereunder

49. The SEC repeats, realleges, and incorporates by reference paragraphs 1 through 45, as though fully set forth therein.

50. Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 13a-1 and 13a-13 thereunder [17 C.F.R. §§ 240.13a-1, 240.13a-13] require issuers of registered securities to file with the SEC factually accurate annual reports (on Form 10-K) and quarterly reports (on Form 10-Q). Exchange Act Rule 12b-20 [17 C.F.R. § 240.12b-20] provides that, in addition to

the information expressly required to be included in a statement or report, there shall be added such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they were made, not misleading.

51. By reason of the conduct described above, Defendant Ashford violated, and unless enjoined will continue to violate, Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, and 13a-13 thereunder [17 C.F.R. §§240.12b-20, 240.13a-1, 240.13a-13]. With regard to the violations of Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, and 13a-13 thereunder, Defendant Ashford acted at least negligently.

PRAYER FOR RELIEF

WHEREFORE, the SEC respectfully requests that the Court enter a Final Judgment:

I.

Finding that Defendant Ashford violated the statutes and rules set forth in this Complaint;

II.

Permanently restraining and enjoining Defendant Ashford from violating, directly or indirectly, Section 17(a)(3) of the Securities Act [15 U.S.C. § 77q(a)(3)] in the offer or sale of any security by the use of any means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly, to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser by, directly or indirectly, (i) creating a false appearance or otherwise deceiving any person concerning a material event, or (ii) disseminating false or misleading documents, materials, or information or making, either orally or in writing, any false or misleading statement in any communication with any investor or prospective investor concerning a material event.

III.

Permanently restraining and enjoining Defendant Ashford from violating, directly or indirectly, Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, and 13a-13 thereunder [17 C.F.R. §§ 240.12b-20, 240.13a-1, 240.13a-13].

IV.

Ordering Defendant to pay civil monetary penalties pursuant to Section 20(d) of the Securities Act [15 U.S.C. § 77t(d)] and Section 21(d)(3) of the Exchange Act [15 U.S.C. § 78u(d)(3)];

V.

Granting such other and further relief as the Court determines to be necessary and appropriate.

VI.

Retaining jurisdiction over this action to implement and carry out the terms of all orders and decrees that may be entered.

JURY TRIAL DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff SEC demands that this case be tried to a jury.

Date: January 13, 2025

Respectfully submitted,

UNITED STATES SECURITIES AND EXCHANGE COMMISSION

/s/Derek Kleinmann
Derek Kleinmann*
Kansas Bar No. 22732
Patrick Disbennett
Texas Bar No. 24094629
United States Securities and Exchange Commission
Fort Worth Regional Office

801 Cherry Street, Suite 1900
Fort Worth, Texas 76102
Tel: (817) 900-2623 (Kleinmann)
kleinmannd@sec.gov
Tel: (817) 266-9633 (Disbennett)
disbennettpa@sec.gov

* pending admission *pro hac vice*