IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BUTTE DIVISION

IN RE: SNOWFLAKE, INC., DATA SECURITY BREACH LITIGATION This Document Relates to Defendant: The Neiman Marcus Group LLC	Case No.: 2:24-MD-3126-BMM

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Marc Reichbart, Jamillah Sherman, Chrystal Pelosi, Anastasia Kouriatova, and Ron Slomowicz ("Plaintiffs") bring this Consolidated Class Action Complaint ("Complaint") against Defendant The Neiman Marcus Group LLC ("Neiman Marcus" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises from a cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant ("Data Breach" or "Data Incident").

2. The Neiman Marcus Group LLC is the parent company of leading U.S. multi-brand luxury retailers Neiman Marcus and Bergdorf Goodman. Neiman

Marcus is an American department store chain focusing on luxury retail incorporating the internationally recognized names of several high-end brands.

3. Defendant requires customers to provide their PII prior to or at the time of purchase. Defendant's website provides "[w]here we require your personal data to complete your purchase transactions, failure to provide such information may result in us being unable to complete your transactions."

4. Occurring on or about, May 20, 2024, the Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former customers' and employees' personally identifying information ("PII" or "Private Information"), including customer name, date of birth, gift card numbers, and transaction details, as well as, for a smaller subset, the last four digits of a Social Security number and miscellaneous employee data.[1]

5. In June 2024, Defendant reported "an unauthorized party gained access to a cloud database platform used by [Neiman Marcus] that is provided by a third party, Snowflake." "The disclosure and the data breach notifications came after a

[1] Neiman Marcus Notice of Data Breach (June 24, 2024) ("Neiman Marcus Notice"), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/f5f736b6-9f8e-4d3f-9d24-d5d14ab9d56f.html (last accessed Apr. 21, 2025); Sead Fadilpašić, *Neiman Marcus confirms data breach, claims its Snowflake account was hacked*, TechRadar (June 26, 2024), https://www.techradar.com/pro/security/neiman-marcus-confirms-data-breach-claims-its-snowflake-account-was-hacked (last accessed Apr. 21, 2025).

threat actor using the 'Sp1d3r' handle put Neiman Marcus' data up for sale on a hacking forum, asking $150,000 for 12 million gift card numbers, 70 million transactions with full customer details, and 6 billion rows of customer shopping records, store information, and employee data."

6. Plaintiffs and proposed Class Members are victims of Defendant's negligence and inadequate cybersecurity measures. Specifically, Plaintiffs and Class Members trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

7. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees.

PARTIES

8. Plaintiff Marc Reichbart is a natural person and citizen of the state of Florida.

9. Plaintiff Jamillah Sherman is a natural person and citizen of the state of New Jersey.

10. Plaintiff Chrystal Pelosi is a natural person and citizen of the state of New Jersey.

11. Plaintiff Anastasia Kouriatova is a natural person and citizen of the state

of California.

12. Plaintiff Ron Slomowicz is a natural person and citizen of the state of Illinois.

13. Defendant The Neiman Marcus Group LLC is a Delaware limited liability company, with its headquarters and principal place of business located at One Marcus Square, 1618 Main Street, Dallas, Texas.

JURISDICTION AND VENUE

14. The Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Defendant is a citizen of a state different from that of at least one Class Member.

15. Venue is proper in this District for pretrial purposes consistent with the process for multidistrict litigation for the reasons set out in the Judicial Panel on Multidistrict Litigation's Transfer Order centralizing actions consolidated in this MDL to the District of Montana. *In re: Snowflake, Inc. Data Sec. Breach Litig.*, MDL No. 3126, 2024 WL 4429233 (J.P.M.L. 2024).

FACTUAL ALLEGATIONS

Neiman Marcus's Business and Data Security Promises.

16. Neiman Marcus is a premium luxury retailer which makes billions of

dollars every year selling high-end fashions,[2] but takes a comparatively cut-rate approach to the data security protocols for its customers' data.

17. While Neiman Marcus collects troves of highly sensitive and intrusive personal information from shoppers online and in its stores, it only uses the most rudimentary "username and password" security to protect access to its customers' most sensitive information. Predictably, this security proved ineffective to deter those with ill intent, and millions of Neiman Marcus customers now find themselves at the mercy of hackers and cybercriminals, who target them with phishing attempts and fraudulent schemes with the extensive data they were able to steal from the high-end retailer.

18. Neiman Marcus promises its customers that the security of their information is one of its paramount concerns:

> We are committed to handling your personal information with high standards of information security. We take appropriate physical, technical, and administrative steps to maintain the security and integrity of personal information we collect, including limiting the number of people who have physical or logical access to your data, as well as employing a multitude of technical controls to guard against unauthorized access. We also routinely train our employees in security

[2] *Neiman Marcus Group Delivers $5 billion of GMV in FY22, Demonstrating Strength of Integrated Luxury Retail Model*, Neiman Marcus Bergdorf Goodman (Oct. 12, 2022), https://www.neimanmarcusgroup.com/2022-10-12-Neiman-Marcus-Group-Delivers-5-billion-of-GMV-in-FY22,-Demonstrating-Strength-of-Integrated-Luxury-Retail-Model (last accessed Apr. 21, 2025).

and compliance best practices.[3]

19. Defendant's Privacy Policy applies to information collected from customers using its website, mobile applications, and from in-store visits. Plaintiffs and Class Members, as customers, relied on these representations and on this sophisticated business entity to keep their PII confidential, securely maintained, and to make only authorized disclosures of this information.

20. While Neiman Marcus makes these promises, it also does so while collecting troves of sensitive data on its customers every time they visit its website or a Neiman Marcus brick-and-mortar store. The type of information varies from name, address, telephone number, birth date, and account number, to geolocation, preferences about products, and videos and photos of individual customers.[4]

21. The trove of data that Neiman Marcus collects on its consumers allows it to build elaborate profiles for each consumer, so that it may identify products that the customer might want to buy.[5] This sophisticated type of marketing has led other retailers to see a 40% increase in revenue.[6] When companies collect this type of data,

---

[3] *Privacy Policy & Terms of Use*, Security & Privacy, assistance.neimanmarcus.com/privacy#securityandprivacy (last accessed Apr. 21, 2025).

[4] *Id.*

[5] *Id.*

[6] *What is personalization?*, McKinsey & Company (May 30, 2023), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-personalization (last accessed Apr. 21, 2025).

however, best practices dictate that implementing "robust security precautions like encryption, access controls and network-level protections" is a "top priority."[7]

22. Neiman Marcus acknowledges that it may provide consumer data to a "service provider," but that it "require[s] that these outside companies agree to keep confidential all information we share with them, use the information only to perform their obligations in our agreements with them, and abide by applicable data privacy laws."[8]

23. Neiman Marcus is fully aware of cybersecurity risks, so much so that it warns its customers to use best practices to keep their own data safe—for example, "using strong, complex and unique passwords," "[u]sing different passwords across online accounts," "[e]nsuring that your mobile devices and computers are updated with the most recent security patches and that you are utilizing virus and other malware protection technologies on those devices," "[n]ot clicking on links and attachments from senders that you do not recognize," "[n]ever providing your credentials or personal information on websites unless you are certain of its

---

[7] Terry Tolentino, *Marketing Data Collection in 2025: Use Cases & Best Practices*, Marketing Scoop (Mar. 17, 2024), https://www.marketingscoop.com/ai/data-collection-for-marketing/ (last accessed Apr. 21, 2025).

[8] Neiman Marcus Privacy Policy and Terms of Use, Security & Privacy, assistance.neimanmarcus.com/privacy#securityandprivacy (last accessed Apr. 21, 2025).

authenticity," and "[r]eviewing your Neiman Marcus account periodically and notifying us of any unusual activity."[9]

24. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

25. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

26. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its customers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

Neiman Marcus Breach Its Duty to Protect PII and Engaged in Unfair Trade Practices.

9 *Id.*

27. Despite Neiman Marcus's explicit assurances that they would safeguard its customers' sensitive PII, it notified customers in June 2024 that, between April and May 2024, an "unauthorized third party gained access to a database platform used by the Neiman Marcus Group."[10]

28. This is not the first time Neiman Marcus has had a data breach. In 2021, it notified customers that "an unauthorized party obtained personal information associated with certain of our customers' online accounts," including names and contact information, payment card numbers and expiration numbers (without CVV numbers), Neiman Marcus virtual gift card numbers (without PINs), and usernames, passwords, and security questions and answers associated with Neiman Marcus accounts.[11]

29. Before that, in 2013, hackers stole 350,000 credit card numbers of its customers before "some of its customers had found fraudulent charges on their cards."12

30. Neiman Marcus was well aware of the security risks that maintaining such information posed, so much so that they should have taken basic cybersecurity

---

[10] Neiman Marcus Notice at 1.

[11] *Important information about customer online accounts*, Neiman Marcus (Sept. 30, 2021), https://www.neimanmarcus.com/editorial/security/online-accounts/ (last accessed Apr. 21, 2025).

[12] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015).

steps to protect it.

31. Indeed, as a result of a prior data breach, Neiman Marcus entered into a settlement agreement, where it agreed to adopt many business practice changes "to further enhance the security of its customers' data." *Remijas v. Neiman Marcus Group, LLC*, No. 14-cv-01735, ECF No. 221-1 (N.D. Ill. Oct. 28, 2019).

32. At the time of the Data Breach, Neiman Marcus failed to maintain reasonable data security measures and comply with FTC guidance, the PCI DSS, and other relevant industry standards summarized above. These data security failings included:

- Neiman Marcus did not enforce MFA for its Snowflake accounts.
- Neiman Marcus did not rotate or disable the credentials of old Snowflake accounts.
- Neiman Marcus did not implement network allow lists that Snowflake account access to certain locations or trusted users.

33. Neiman Marcus failed to take these measures despite being under constant attacks and attempted attacks from threat actors. Its failure to implement these measures led to the Data Breach, as each of the protections outlined above could have prevented the Data Breach.

34. Neiman Marcus's basic data security failings also breached its duty of care to protect the PII of consumers.

PII Stolen About Plaintiffs and Class Members

35. Neiman Marcus announced that, based upon its investigation of the Data Breach, "the unauthorized third party obtained certain personal information stored in the database platform. The types of personal information affected varied by individual, and included information such as name, contact information, date of birth, and Neiman Marcus or Bergdorf Goodman gift card number(s) (without gift card PINs)."13

36. Beyond Neiman Marcus's public disclosure, it is likely that the Data Breach extended far beyond the information identified above. In June 2024, the threat actor Sp1d3r posted stolen data for sale on the dark web for $150,000, including:

- Name, address, phone number, date of birth, email, last four of Social Security number, "and much more."
- 70 million transactions (with "full customer details, last 4 of SSN, and more").
- 50 million customer email addresses with IP addresses.
- 12 million gift card numbers ("with name, gift card number, balances, and more").
- 6 billion rows of customer shopping records, employee data, and store information.[14]

---

13 Notice Letter.

14 HacManac Post: Major #DataBreach (June 25, 2024), https://x.com/H4ckManac/status/1805480891134697655 (last accessed Apr. 21, 2024).

37. Based upon an independent review of the information, at least 30 million unique email addresses appear in the data set, which has been confirmed with multiple individuals whose data was in the stolen database.[15]

38. The information posted for sale closely matches the type of information Neiman Marcus regularly collects on its shoppers, allowing it to create individualized profiles on shoppers to target them with sophisticated marketing strategies.

The Data Breach Was a Foreseeable Risk of which Defendant Was on Notice.

39. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches among retailers preceding the date of the breach.

40. In light of recent high profile data breaches at other retailers, Defendant knew or should have known that its electronic records and customers' PII would be targeted by cybercriminals.

41. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from

[15] Sergiu Gatlan, *Neiman Marcus data breach: 31 million email addresses found exposed*, BLEEPINGCOMPUTER (July 8, 2024), https://www.bleepingcomputer.com/news/security/neiman-marcus-data-breach-31-million-email-addresses-found-exposed/ (last accessed Apr. 21, 2024).

2020.[16] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[17]

42. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft.

43. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

44. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, and lost time. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

---

[16] 2021 Data Breach Annual Report, ITRC, https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last accessed Apr. 21, 2024).

[17] *Id*.

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

45. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

46. The value of Plaintiffs' and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" Internet

websites, making the information publicly available, for a substantial fee of course.

47. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

48. One such example of criminals using PII for profit is the development of "Fullz" packages.

49. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

50. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen

PII is being misused, and that such misuse is fairly traceable to the Data Breach.

51. Defendant disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

52. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Failed to Adhere to FTC Guidelines.

53. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

54. In 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established guidelines for fundamental data security principles

and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

55. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

56. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders

resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers, and in this case, its customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

59. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

60. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

61. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and

limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

62. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

63. These foregoing frameworks are existing and applicable industry standards for an employer and company's obligations to provide adequate data security for its employees and customers. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Plaintiff Marc Reichbart's Experiences

64. Plaintiff Marc Reichbart (for purposes of this section, "Plaintiff") is

a customer of Neiman Marcus, where he provided it with personal information, including at least his name, address, and email.

65. Since the Data Breach, Plaintiff has experienced an increase in spam, and has noticed an uptick in scam emails and receives several such emails per week. Since the Data Breach, Plaintiff has spent approximately hours investigating and mitigating against the substantial risks presented by the theft of his PII. These mitigation efforts have included reviewing financial account statements, and monitoring his credit reports.

66. As a result of the Data Breach, Plaintiff has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent utilizing credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property with respect to the inability to control use of his PII; invasion of his privacy; and anxiety resulting from the theft of his PII.

67. Plaintiff is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the Internet or any other unsecured source. Plaintiff stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, Plaintiff diligently chooses unique

usernames and passwords for his various online accounts.

Plaintiff Jamillah Sherman's Experiences

68. Plaintiff Jamillah Sherman (for purposes of this section, "Plaintiff") is a customer of Neiman Marcus, where she provided it with personal information, including at least her name, address, and email.

69. Since the Data Breach, Plaintiff has experienced an increase in spam, and has noticed an uptick in scam emails and receives several such emails per week. Since the Data Breach, Plaintiff has spent approximately hours investigating and mitigating against the substantial risks presented by the theft of her PII. These mitigation efforts have included reviewing financial account statements, and monitoring her credit reports.

70. As a result of the Data Breach, Plaintiff has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent utilizing credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property with respect to the inability to control use of her PII; invasion of her privacy; and anxiety resulting from the theft of her PII.

71. Plaintiff is very careful about sharing her own PII and has never knowingly transmitted unencrypted PII over the Internet or any other unsecured source. Plaintiff stores any and all documents containing PII in a secure location

and destroys any documents she receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

Plaintiff Chrystal Pelosi's Experiences

72. Plaintiff Chrystal Pelosi (for purposes of this section, "Plaintiff") is a customer of Neiman Marcus, where she provided it with personal information, including at least her name, address, and email.

73. Since the Data Breach, Plaintiff has experienced an increase in spam, and has noticed an uptick in scam emails and receives several such emails per week. Since the Data Breach, Plaintiff has spent approximately hours investigating and mitigating against the substantial risks presented by the theft of her PII. These mitigation efforts have included reviewing financial account statements, and monitoring her credit reports.

74. As a result of the Data Breach, Plaintiff has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent utilizing credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property with respect to the inability to control use of her PII; invasion of her privacy; and anxiety resulting from the theft of her PII.

75. Plaintiff is very careful about sharing her own PII and has never knowingly transmitted unencrypted PII over the Internet or any other unsecured source. Plaintiff stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

Plaintiff Anastasia Kouriatova's Experiences

76. Plaintiff Anastasia Kouriatova (for purposes of this section, "Plaintiff") is a customer of Neiman Marcus, where she provided it with personal information, including at least her name, address, and email.

77. In June 2024, Plaintiff was informed by Identity Defense that her email address was found on the dark web as a result of the Neiman Marcus data breach. Since the Data Breach, Plaintiff has received approximately 20 additional alerts notifying her that her PII was found on the dark web. Since the Data Breach, Plaintiff has experienced an increase in spam and receives approximately 1-2 spam calls and 1-2 spam messages a day. Since the Data Breach, Plaintiff has also noticed an uptick in scam emails and receives several such emails per week, including one email from a fraudulent actor attempting to sign her up for student loans and another attempting to extort bitcoin from her, claiming they had

recorded her on her webcam.

78. Since the Data Breach, Plaintiff has spent approximately 20-30 hours investigating and mitigating against the substantial risks presented by the theft of her PII. These mitigation efforts have included maintaining her credit freeze with credit agencies, reviewing financial account statements, and monitoring her credit reports.

79. As a result of the Data Breach, Plaintiff has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent utilizing credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property with respect to the inability to control use of her PII; invasion of her privacy; and anxiety resulting from the theft of her PII.

80. Plaintiff is very careful about sharing her own PII and has never knowingly transmitted unencrypted PII over the Internet or any other unsecured source. Plaintiff stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

Plaintiff Ron Slomowicz's Experiences

81. Plaintiff Ron Slomowicz (for purposes of this section, "Plaintiff") is a customer of Neiman Marcus where he provided it with personal information, including at least his name, address, and email

82. Since the Data Breach, Plaintiff has experienced an increase in spam, and has noticed an uptick in scam emails and receives several such emails per week. Since the Data Breach, Plaintiff has spent approximately hours investigating and mitigating against the substantial risks presented by the theft of his PII. These mitigation efforts have included reviewing financial account statements, and monitoring his credit reports.

83. As a result of the Data Breach, Plaintiff has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent utilizing credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property with respect to the inability to control use of his PII; invasion of his privacy; and anxiety resulting from the theft of his PII.

84. Plaintiff is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the Internet or any other unsecured source. Plaintiff stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise his

identity and financial accounts. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

CLASS ACTION ALLEGATIONS

85. Plaintiffs bring this class action under the Federal Rules of Civil Procedure 23(a) and (b)(3) individually and on behalf of all members of the following class:

> All persons who live in the United States whose Personal Information was potentially compromised as a result of the Data Incident.

86. Excluded from the Class are all persons who are governing board members of Defendant, governmental entities, the Court, and Court's immediate staff.

87. Plaintiffs reserve the right to amend or modify the definition of the Class or create additional subclasses as this case progresses.

88. **Numerosity**. The members of the Class are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that Neiman Marcus acknowledged that 64,472 individuals were compromised in the Data Breach, with cybersecurity experts identifying millions more.

89. **Commonality.** There are questions of fact and law common to the Class, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

- Whether Neiman Marcus had a duty to protect the Personal Information of Plaintiffs and Class Members.
- Whether Neiman Marcus breached express or implied commitments to protect the Personal Information of Plaintiffs and Class Members.
- Whether Neiman Marcus knew or should have known that its data security practices were deficient.
- Whether Neiman Marcus's data security systems were consistent with industry standards prior to the Data Breach.
- Whether Neiman Marcus adequately disclosed details regarding the Data Breach to affected consumers.
- Whether Neiman Marcus unlawfully utilized, retained, misplaced, or exposed Plaintiffs' and the Class Members' Personal Information.
- Whether Plaintiffs and Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, general damages, nominal damages, and/or injunctive relief.

90. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Personal Information, like that of every other Class Member, was compromised in the Data Breach

91. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interest of Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

92. **Predominance.** Neiman Marcus has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the data of Plaintiff and

Class Members were stored on the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from Neiman Marcus's conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

93. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Class. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Neiman Marcus Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Neiman Marcus. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Neiman Marcus Class Member.

94. **Injunctive Relief.** Neiman Marcus has acted on grounds that apply generally to the Neiman Marcus Class as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a classwide basis.

95. **Issue Certification.** Likewise, particular issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such particular issues include, but are not limited to:

- Whether Neiman Marcus owed a legal duty to Plaintiffs and Class Members to protect their Personal Information.
- Whether Neiman Marcus's data security measures were inadequate in light of applicable regulations and industry standards.
- Whether Neiman Marcus's data security measures were negligent.
- Whether Neiman Marcus breached express or implied representations to Plaintiffs and Class Members regarding the protection of their Personal Information.

96. **Identification of Class Members Using Objective Criteria.** Finally, all members of the proposed Class are readily identifiable using objective criteria. Neiman Marcus has access to the names and contact information of Class Members affected by the Data Breach, and cybersecurity professionals have already analyzed dark web data to identify class members by email address. Adequate notice can be given to Class members directly using information maintained in Defendant's records or via email.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

97. Plaintiffs reallege paragraphs 1 through 96 as if fully set forth below.

98. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

99. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

100. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if their PII was wrongfully disclosed.

101. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' PII.

102. Defendant owed—to Plaintiffs and Class members—at least the

following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access; and

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII.

103. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

104. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

105. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and

the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

106. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment from Defendant.

107. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class members' PII.

108. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' PII.

109. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had

collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

111. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

112. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendant breached these duties as evidenced by the Data Breach.

114. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs and Class members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used,

and exchanged, and those in its employ who were responsible for making that happen.

115. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs and Class members' injury.

116. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class members' injuries-in-fact.

117. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

118. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages.

119. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without

limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

120. Plaintiffs reallege paragraphs 1 through 96, as if fully set forth below.

121. Plaintiffs and the Class delivered their PII to Defendant as part of the process of obtaining treatment and services provided by Defendant.

122. Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiffs' and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

123. In providing their PII, Plaintiffs and Class Members entered into an

implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' PII.

124. In delivering their PII to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard that data.

125. Plaintiffs and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

126. Defendant accepted possession of Plaintiffs' and Class Members' PII.

127. Had Defendant disclosed to Plaintiffs and Class Members that Defendant did not have adequate computer systems and security practices to secure customers' PII, Plaintiffs and members of the Class would not have provided their PII to Defendant.

128. Defendant recognized that customers' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

129. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

130. Defendant breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard its data.

131. Defendant breached the implied contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

132. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII; and (g) the continued and substantial risk to Plaintiffs' and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiffs' and Class Members' PII.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

133. Plaintiffs reallege paragraphs 1 through 96, as if fully set forth below.

134. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

135. Plaintiffs and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

136. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's PII, as this was used to facilitate the treatment, services, and goods it sold to Plaintiffs and the Class.

137. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs and the Class's PII because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII to Defendant had they known Defendant would not adequately protect their PII.

138. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the

proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: May 2, 2025

Respectfully submitted,

By: */s/ Jason S. Rathod*

Jason S. Rathod
Migliaccio & Rathod LLP
412 H St NE, Suite 302
Washington DC 20002
Tel. 202.470.3520
jrathod@classlawdc.com

Attorneys for Plaintiffs and the Putative Class