IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

MARC REICHBART, individually and on behalf of all others similarly situated, ***Plaintiff,*** **vs.** **NEIMAN MARCUS GROUP LLC, and SNOWFLAKE, INC.,** ***Defendants.***	**Civil Action No.:** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Marc Reichbart ("Plaintiff") brings this Class Action Complaint against Neiman Marcus Group LLC, ("Defendant") and Snowflake Inc., ("Snowflake") individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

STATEMENT OF FACTS

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the personally identifiable information (PII) of its customers, including, but not limited to: names, emails, addresses, phone numbers, dates of birth, last four digits of Social Security numbers, credit card numbers, transaction data, and employee identification numbers.

2. 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. Snowflake is a cloud storage services vendor retained by Defendant. The Neiman Marcus data breach is part of a large-scale hacking campaign affecting hundreds of Snowflake's customers.

4. 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."

5. On, or about, May 20, 2024, Plaintiff's and Class Members' personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against unauthorized disclosure—was compromised in a data breach (hereafter referred to as, the "Data Breach"). The Data Breach included personal details of about 31million customers.

6. The PII compromised in the Data Breach was exfiltrated by cyber-criminals who target PII for its value to identity thieves. ShinyHunters, the hacker group claiming responsibility for the Data Breach, has been linked to a string of high-profile data breaches resulting in millions of dollars in losses.[1]

7. In June 2024, Defendant reported "an unauthorized party gained access to a cloud database platform used by [Neiman Marcus Group] that is provided by a third party, Snowflake."[2] "The disclosure and the data breach notifications came after a threat actor using the 'Sp1d3r' handle put Neiman Marcus' data up for sale on a hacking forum, asking $150,000 for 12 million

[1] *See*, *Data allegedly stolen from 560 million Ticketmaster users*, https://www.bbc.com/news/articles/c899pz84d8zo (accessed June 11, 2024).
[2] https://www.bleepingcomputer.com/news/security/neiman-marcus-data-breach-31-million-email-addresses-found-exposed (last accessed July 17, 2024).

gift card numbers, 70 million transactions with full customer details, and 6 billion rows of customer shopping records, store information, and employee data."[3]

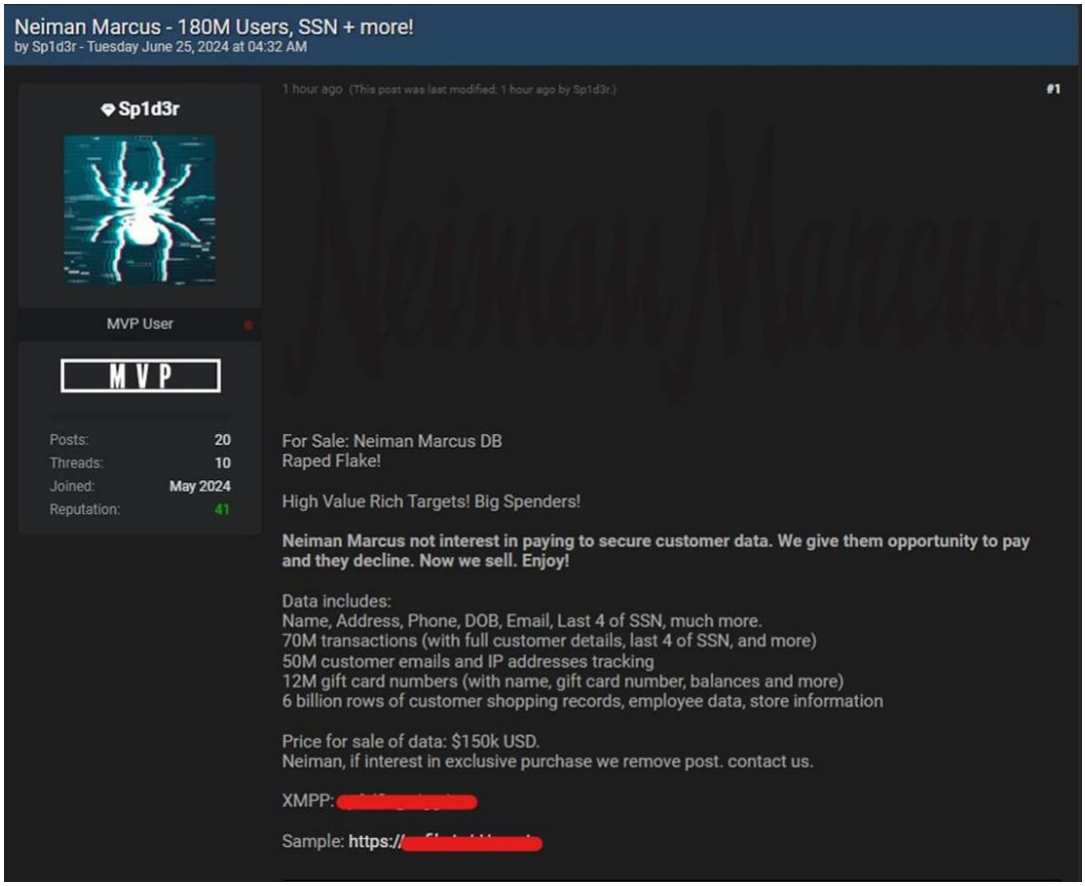

**image of stolen data posted for sale on hacking forum*

8. Earlier this year, cybercriminals figured out that many major companies have uploaded massive amounts of valuable and sensitive customer data to Snowflake servers. The threat actors responsible for the Data Breach targeted Defendant due to its failure to configure multi-factor authentication (MFA) to protect the cloud database.

9. Defendant promised to use reasonable technical and administrative safeguards to protect the PII it collected. These promises were contained in the applicable privacy policy, its website, and through other disclosures in compliance with statutory privacy requirements.

[3] *Id.*

10. For example, Defendant's Privacy Policy provides, in relevant part, "[w]e 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 and compliance best practices."[4]

11. Defendant's Privacy Policy also provides that PII may be shared with "service providers," which are outside companies that help Defendant deliver its products and services. Service providers include companies retained to: (i) manage a database of customer information; (ii) assist with marketing and data collection; (iii) provide storage and analysis; and (iv) provide other services designed to maximize business potential. Defendant represents that it requires "these outside companies [ ] to keep confidential all information [shared] with them, . . . and abide by applicable data privacy laws."[5]

12. Defendant's Privacy Policy applies to information collected from customers using its website, mobile applications, and from in-store visits. Plaintiff and Class Members (later defined) are current and former customers of Defendant. Plaintiff 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.

---

[4] *Privacy Policy & Terms of Use*, https://assistance.neimanmarcus.com/privacy?itemId=cat33940739#securityandprivacy (last accessed July 17, 2024).

[5] *Privacy Policy & Terms of Use*, https://assistance.neimanmarcus.com/privacy?itemId=cat33940739#securityandprivacy (last accessed July 17, 2024).

13. Defendant acknowledges that it is responsible for protecting its customers' privacy.[6] However, Defendant completely and utterly failed to protect its customers' personal data and/or ensure that technical controls were implemented to prevent unauthorized access to the cloud database containing customer data and/or implement appropriate technical and administrative actions to maintain the security of the customer data Defendant stored in the cloud database.

14. Defendant did not notify Plaintiff of the Data Breach until June 24, 2024. Omitted from the data breach notice letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff, who retains a vested interest in ensuring that their PII remains protected.

15. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take the necessary steps to secure the PII from those risks left the data in a dangerous condition.

16. The Data Breach was a direct result of Defendant's (or Snowflake's) failure to implement reasonable safeguards to protect PII from a foreseeable and preventable risk of unauthorized disclosure. Had Defendant implemented reasonable administrative, technical, and/or physical controls consistent with industry standards and its own Privacy Policy, the Data Breach would have been prevented.

17. Defendant's (or Snowflake's) conduct resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals. The unauthorized disclosure of Plaintiff's PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's

[6] *See*, Section XIII, *Data Controller*, Privacy Policy & Terms of Use.

(or Snowflake's) failure to adequately secure the PII in its custody (or under its control), and has resulted in actual, particularized, and concrete harm to the Plaintiff. Plaintiff suffered actual injury in the form of damages to and diminution in the value of the PII that was compromised as a result of the Data Breach. The injuries Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

18. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

19. Defendant's (or Snowflake's) conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft, fraud, or other forms of exploitation. The circumstances demonstrating a substantial risk of future exploitation include, but are not limited to:

a. **Data Type**: The data acquired in the Data Breach included unencrypted names, emails, addresses, phone numbers, dates of birth, last four digits of Social Security numbers, credit card numbers, transaction data, and employee identification numbers, which can be used to perpetuate fraud, identity theft, and other types of exploitation. The stolen data can be used to identify key relationships, pinpoint vulnerabilities, and craft highly sophisticated social engineering-based attacks. A social engineering attack is a method of using psychological manipulation to deceive a victim and gain access to a computer system or to steal sensitive information such as login credentials. Social engineering attacks that can be launched using names, telephone numbers and email addresses include phishing, smishing (SMS message), vishing (voice messaging), pretexting, and baiting attacks. This data can also be used in SIM swapping scams and port-out fraud.[7]

b. **Data Breach Type**: This was a targeted attack, orchestrated by a hacker that is, upon information and belief, part of the ShinyHunters hacking group. ShinyHunters has been linked to a string of high-profile data breaches resulting in millions of dollars in losses. In 2021, ShinyHunters stole a database of personal information regarding 70 million consumers and then sold the data on the dark web.[8] Furthermore, since 2020, ShinyHunters has stolen over 900 million customer

[7] https://www.ccmi.com/fcc-will-update-cpni-rules-to-stop-data-breaches/ (last accessed May 21, 2024).
[8] *See*, *Data allegedly stolen from 560 million Ticketmaster users*, https://www.bbc.com/news/articles/c899pz84d8zo (accessed June 11, 2024).

records in a series of high-profile data breaches (*e.g.*, GitHub, AT&T, Ticketmaster, Pizza Hut). Upon information and belief, ShinyHunters has accumulated enough personal information from that series of data breaches to be able to commit identity theft, fraud, or other forms of exploitation against Plaintiff and Class Members.

c. **Data Misuse**: The hacker responsible for the Data Breach leaked the data it acquired in the Data Breach on the dark web. The dark web uses a series of encrypted networks to hide users' identities, which makes it convenient for criminals to buy and sell illegally obtained data. Many criminals purchase stolen personal data off the dark web before launching social engineering-based attacks.

20. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PII in its custody (or under its control), and has created a separate, particularized, and concrete harm to the Plaintiff.

21. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused them to: (i) spend money on mitigation measures like credit monitoring services and/or dark web scans and monitoring; (ii) lose time and effort spent responding to the Data Breach, like finding where the data is exposed and at risk; (iii) spend money removing data from risky databases or deleting it from data broker databases; and/or (iv) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff suffered can be redressed by a favorable decision in this matter.

22. Plaintiff faces a substantial risk of future spam, phishing, or other social engineering attacks where full names, addresses, email addresses, and phone numbers can be readily accessed by cybercriminals, known for stealing and reselling personal data on the dark web.

23. The exposure of the PII involved in this data breach is particularly alarming because threat actors may use the data to circumvent SMS-based multifactor authentication security measures by intercepting multifactor authentication codes sent via text. Therefore, Plaintiff and

Class Members must incur out of pocket costs for purchasing products to protect from phishing, smishing (SMS message), vishing (voice messaging), pretexting, and other sophisticated attacks.

This Data Breach Was Avoidable

24. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[9] Ransomware groups frequently implement a double extortion tactic, "where the cybercriminal posts portions of the data to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[10]

25. To prevent and detect data breaches of the type at issue here, Defendant and/or Snowflake could and should have implemented, at least, the following measures and/or ensured its cloud-services vendors implemented the following measures:

Reasonable technical and administrative data protection measures

a. Identify the computers or servers where sensitive personal information is stored.
b. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices.
c. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.
d. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

[9] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).
[10] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).

e. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[11]

26. ISO/IEC 27017 provides guidance on multi-factor authentication (MFA) as a security control for cloud service customers. The standard provides, among other things, the following security requirements:

a. **Authentication Requirements**: The standard emphasizes the importance of strong authentication mechanisms for accessing cloud services. It recommends the use of MFA as an effective method to enhance the security of user authentication. MFA requires users to provide multiple forms of identification, such as a password and a unique code or biometric factor, to verify their identity.

b. **Risk Assessment**: ISO/IEC 27017 encourages cloud service customers to conduct a risk assessment to determine the level of authentication controls required based on the sensitivity of the data and the potential impact of unauthorized access. MFA is often recommended for high-risk or sensitive applications or data.

c. **Access Controls**: The standard provides guidance on implementing access controls in the cloud environment. It suggests that MFA should be used as an additional layer of security in conjunction with other access control measures such as strong passwords, role-based access control (RBAC), and least privilege principles.

d. **User Management**: ISO/IEC 27017 highlights the need for effective user management practices in the cloud. It recommends implementing MFA for user accounts with administrative privileges or access to sensitive data. This helps prevent unauthorized access even if the user's password is compromised.

e. **Supplier Management**: The standard advises cloud service customers to assess the authentication capabilities of their cloud service providers. It recommends selecting providers that offer robust MFA options and have appropriate controls in place to protect customer data.

f. **Compliance Monitoring**: ISO/IEC 27017 suggests that organizations should monitor and review the effectiveness of their MFA controls regularly. This includes monitoring user access logs, analyzing authentication success/failure rates, and promptly addressing any security incidents or vulnerabilities related to authentication.

[11] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

27. By addressing MFA in these ways, cloud service customers like Defendant can strengthen their authentication processes, reduce the risk of unauthorized access, and enhance the overall security of their cloud services.

28. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and Class Members' PII.

29. Defendant knew and understood unencrypted PII is valuable and highly sought after by cybercriminals. Considering Defendant's target market includes affluent clientele and consumers of luxury goods, Defendant knew, or reasonably should have known, of the importance of safeguarding customer PII in cloud environments and of the foreseeable consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and Class Members as a result.

30. Furthermore, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) adhere to its published privacy practices; (iii) implement identity and access management (IAM) policies and technology to ensure that the correct users have the appropriate access to technology resources; (iv) implement multifactor authentication in cloud environments and require users to provide more than one form of identification before accessing systems, applications, or services; (v) implement reasonable data protection measures for the collection, use, disclosure, and storage of personal information; and/or (vi) ensure its third-party vendors were required to

implement reasonable data protection measures consistent with Defendant's data protection obligations.

Plaintiff and Class Members Sustained Damages in the Data Breach

31. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct. As a consequence of the Data Breach, Plaintiff and Class Members sustained monetary damages that exceed the sum or value of $5,000,000.00.

32. Armed with the PII acquired in the Data Breach, data thieves have already engaged in theft, have already misused the data by posting it on the dark web, and now the data can be used to commit other forms of exploitation in the future.

33. As a result of the Data Breach, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

34. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz"

packages.[12] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

35. Given the type of targeted attack in this case, the sophistication of the criminal claiming responsibility for the Data Breach, the type of PII involved in the Data Breach, the hacker group's behavior in prior data breaches, the ability of criminals to link data acquired in the Data Breach with information available from other sources, and the fact that the stolen information has been shared on the dark web, it is reasonable for Plaintiff and the Class Members to assume that their PII was obtained by, or released to, criminals intending to utilize the PII for future identity theft-related crimes or exploitation attempts.

36. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

37. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts

[12] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package typically includes the victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm

opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[13]

38. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year.

39. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and illegitimate markets, has been damaged and diminished by its unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

40. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[14] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[15] Sensitive PII can sell for as much as $363 per record.[16]

---

[13] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

[14] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[15] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[16] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

41. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members, collecting their PII, using their PII for profit or to improve the ability to make profits, and then permitting the unauthorized disclosure of the PII, Plaintiff and Class Members were deprived of the benefit of their bargain.

42. When agreeing to pay Defendant for products or services, consumers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendant did not invest the funds into implementing reasonable data security practices. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

43. Plaintiff brings this class action lawsuit to address Defendant's inadequate data protection practices and for failing to provide timely and adequate notice of the Data Breach.

44. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff has a continuing interest in ensuring that personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

PARTIES

45. Plaintiff Marc Reichbart is an adult citizen of the State of Florida. At all relevant times, Plaintiff Reichbart has been a resident of Lakewood, Walton County, Florida. Plaintiff Reichbart received a data breach notice letter from Defendant in July 2024. Plaintiff has noticed an increase in spam calls, texts and/or emails since the occurrence of the Data Breach.

46. Defendant, Neiman Marcus Group LLC is a Delaware limited liability company with its principal office or place of business at 1618 Main Street Dallas, Texas 75201 (Dallas

County). Defendant is the parent company of Neiman Marcus, a leading luxury brand retailer with physical stores and an online presence at https://www.neimanmarcus.com. Defendant is registered to do business in the State of Florida and its registered agent for service of process is CT Corporation System, 1200 South Pine Island Road, Plantation, Florida 33324 (Broward County).

47. Defendant Snowflake is a Delaware corporation with its principal office or place of business located at 106 E. Babcock Street, Suite 3A, Bozeman, Montana 59715. Snowflake is registered to do business in the State of Florida and its registered agent for service of process is Corporation Service Company, 1201 Hays Street, Tallahassee, Florida 32301(Leon County).

48. Defendant Neiman Marcus, as the data controller[17], determined the purposes for which and the means by which the PII at issue in this suit was processed. Snowflake is a data processor because it is the third-party who processed the PII on behalf of Defendant Neiman Marcus. As the data controller, Defendant Neiman Marcus is responsible for the negligence of its processors, including Snowflake; thus, any and all allegations herein against Defendant Neiman Marcus are also imputed to Snowflake. Plaintiff reserves the right to amend the Complaint to include additional claims and allegations against Snowflake to conform to the facts revealed through discovery.

JURISDICTION & VENUE

49. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from each Defendant.

[17] *See*, Section XIII, *Data Controller*, Privacy Policy & Terms of Use.

50. This Court has personal jurisdiction over Defendants because Defendants have purposefully availed themselves of the laws, rights, and benefits of the forum state by registering to do business, paying taxes, operating retail chains, and selling products or services within this District. Jurisdiction in this District is proper because the claims against both Defendants are part of the same case or controversy and arise out of or relate to one of the Defendant's contacts within the forum.

51. Venue is proper under 28 U.S.C §1391(b) because Defendants are registered to do business within the forum, Defendants purposefully directed their activities at residents of the forum, this litigation results from alleged injuries that arise out of or relate to those activities, and Defendants are subject to personal jurisdiction in this District.

CLASS ALLEGATIONS

52. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

53. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class:** All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of a data breach that was reported by Defendant in or around June 24, 2024 (the "Class").
>
> **Florida Subclass:** All individuals residing in Florida whose PII was accessed and acquired by an unauthorized party as a result of a data breach that was reported by Defendant in or around June 24, 2024 (the "Florida Subclass").

54. Collectively, the Class and Florida Subclass are referred to as the "Classes" or "Class Members."

55. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

56. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

57. Numerosity: The members of the classes are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of class members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, millions of individuals were impacted in the Data Breach.

58. Common questions of law and fact exist as to all members of the classes and predominate over any questions affecting solely individual members of the classes. The questions of law and fact common to the classes that predominate over questions which may affect individual class members, includes the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
c. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
d. Whether Defendant required its third-party vendors to adequately safeguard the PII of Plaintiff and Class Members;
e. When Defendant actually learned of the Data Breach and the total number of individuals affected thereby;
f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the practices, procedures, or vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

59. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

60. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate for the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenges of these policies hinge on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

61. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

62. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other

available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

63. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

64. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

65. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

66. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Classes, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

67. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

68. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;
c. Whether Defendant's (or their vendors') security measures to protect its network were reasonable in light of industry best practices;
d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;
f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and
g. Whether adherence to recommendations and best practices or other relevant industry standards for protecting personal information in cloud environments would have reasonably prevented the Data Breach.

CAUSES OF ACTION
(*On behalf of Plaintiff and the Classes*)

COUNT 1: NEGLIGENCE/NEGLIGENCE *PER SE*

69. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

70. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

71. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

72. Defendant had full knowledge of the types of PII it collected and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

73. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII for commercial gain, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

74. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology and/or cloud environments; (ii) contractually obligated its vendors to adhere to the requirements of Defendant's privacy policy and applicable laws; (iii) complied with applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits of Defendant's and/or its vendors' data processing activities; (v) regularly audited vendors for compliance with contractual and other applicable data protection obligations; (vi)

provided timely notice to individuals impacted by a data breach event; and (vii) all employees and contractors adhered to the Defendant's Privacy Policy.

75. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies.

76. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII that Defendant was no longer required to retain.

77. Defendant had a duty to take reasonable measures to protect and secure data in electronic form containing personal information. Fla. Stat. §501.171(2).

78. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any fraudulent usage of their PII.

79. Defendant violated Section 5 of the FTC Act by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiff's and Class Members information. Defendant further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII. Defendant's violations of Section 5 of the FTC Act, and other state consumer protection statutes, constitutes negligence *per se.*

80. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to implement organizational controls, including multifactor authentication in cloud environments.

b. Failing to encrypt personally identifying information in transit and at rest.

c. Failing to adopt, implement, and maintain adequate security measures to safeguard PII.

d. Failing to adequately monitor the security of their cloud services vendors.

e. Allowing unauthorized access to PII.

f. Failing to detect in a timely manner that PII had been compromised.

g. Failing to remove former customers' PII it was no longer required to retain.

h. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

i. Failing to implement data security practices consistent with its published privacy policies and standards.

81. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

82. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures was reasonably foreseeable.

83. Plaintiff and the Classes were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of strong authentication mechanisms for accessing cloud services.

84. Plaintiff and the Classes had no ability to protect the PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

85. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure to implement reasonable security measures to protect PII and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

86. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

87. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

88. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and credit monitoring to all affected by the Data Breach.

COUNT 2: BREACH OF IMPLIED CONTRACT

89. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

90. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

91. Defendant published a Privacy Policy to inform the public about how Defendant collects, uses, shares, and protects the information Defendant gathers in connection with the provision of those products or services.

92. In so doing, Plaintiff and Class Members entered implied contracts with Defendant by which Defendant agreed to use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information it collects and stores.

93. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of an expressed or implied promise to implement reasonable data protection measures.

94. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant.

95. Defendant breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on the Defendant's website, privacy policy, and in other documents, all of which created a reasonable expectation that the personal information Defendant collected would be adequately protected and that the Defendant would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

96. As a direct and proximate result of the Defendant's breach of an implied contract, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to

further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

97. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and credit monitoring to all affected by the Data Breach.

COUNT 3: UNJUST ENRICHMENT

98. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

99. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

100. By providing their PII, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant used the PII to market, advertise, and sell additional services to Plaintiff and Class Members. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit.

101. By collecting the PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

102. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

103. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their

PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

104. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT 4: INVASION OF PRIVACY

105. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

106. Plaintiff and Class Members had a legitimate expectation of privacy in their personally identifying information. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

107. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

108. Defendant permitted the public disclosure of Plaintiff's and Class Members' PII to unauthorized third parties.

109. The PII that was disclosed without the Plaintiff's and Class Members' authorization was private and confidential. The public disclosure of the type of PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

110. Defendant permitted its information technology environment to remain vulnerable to foreseeable threats, which created an atmosphere for the Data Breach to occur. Despite knowledge of the substantial risk of harm created by these conditions, Defendant intentionally disregarded the risk, thus permitting the Data Breach to occur.

111. By permitting the unauthorized disclosure, Defendant acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PII at issue was not newsworthy or of any service to the public interest.

112. Defendant was aware of the potential of a data breach and failed to adequately implement appropriate policies and procedures to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

113. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

114. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT 5: VIOLATION OF FLORIDA'S DECEPTIVE & UNFAIR TRADE PRACTICES ACT (Fla. Stat. §§501.201 *et seq*.)

115. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

116. Plaintiff and Class Members are consumers of Defendant's products and services.

Defendant requires its customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

117. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

118. Under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies. Such behavior by Defendant also constitutes a false, misleading, or deceptive act under Florida's Unfair and Deceptive Trade Practices Act. *See,* Fla. Stat. §501.204(2).

119. Defendant violated Fla. Stat. §§501.201 *et seq.*, by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiff's and Class Members' information. Defendant further violated the state consumer protection statute by failing to use reasonable measures to protect PII.

120. Defendant's unfair or deceptive acts affected public interests, including those of Plaintiff and Class Members. Defendant knew or should have known that it was likely to mislead its customers who were acting reasonably. Defendant engaged in unfair or deceptive practices by breaching its duties to provide technical and organizational data security policies, procedures, and practices. Defendant's failure to adhere to its published privacy policies and procedures is offensive to established public policy and is substantially injurious to consumers as evidenced by the massive Data Breach.

121. Had Plaintiff and Class Members known Defendant would not follow its own

published security practices they would not have purchased (or continued to purchase) Defendant's products or services. Defendant's deceptive acts, as described herein, proximately caused Plaintiff and Class Members damages.

122. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered damages including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) mitigation costs and expenses; and (viii) attorneys' fees and court costs.

123. Defendant's data security measures remain inadequate. Plaintiff and Class Members have suffered irreparable injury, and will continue to suffer injury in the future, as a result of Defendant's deceptive trade practices, which places Plaintiff and Class Members at imminent risk that further compromises of their PII will occur in the future. As such, the remedies available at law are inadequate to compensate for that injury. Accordingly, Plaintiff and Class Members also seek to obtain a declaratory judgment that the Defendant's acts or practices violate the act.

124. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

125. The issuance of the requested injunction will not do a disservice to the public

interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose PII would be at risk of future unauthorized disclosures.

126. As a result of the Defendant's false, misleading, or deceptive acts, regarding its data security practices, the consuming public in general, Plaintiff, and Class Members suffered injuries including, but not limited to, the future and continued risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

127. Plaintiff and Class Members are entitled to attorneys' fees, costs, and injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and/or credit monitoring to all affected by the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring each Defendant's conduct violates the statutes and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. Ordering the Defendant to pay for lifetime credit monitoring and dark web monitoring services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: August 1, 2024.

By: */s/ Andrew J. Shamis*
Andrew J. Shamis, Esq.
SHAMIS GENTILE
14 NE 1st Avenue Suite 705
Miami, Florida 33132
Telephone: (305) 479-2299
Fax: (786) 623-0915
Email: ashamis@shamisgentile.com

-AND-

Paul J. Doolittle, Esq.*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com

cmad@poulinwilley.com

Attorneys for Plaintiff

**Pro Hac Vice forthcoming*

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MARC REICHBART, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff WALTON COUNTY, FL
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Shamis & Gentile, PA
14 NE 1st Ave., Suite 705, Miami, FL 33132

DEFENDANTS

NEIMAN MARCUS GROUP LLC, and SNOWFLAKE, INC.,

County of Residence of First Listed Defendant DALLAS, TX
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332

Brief description of cause:
NEGLIGENCE AND NEGLIGENCE PER SE,BREACH OF IMPLIED CONTRACT, UNJUST ENRICHMENT, INVASION OF PRIVACY, VIOLATION

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
AUGUST 1, 2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ Andrew J Shamis

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

MARC REICHBART, individually and on behalf of all others similar situated,

Plaintiff(s)

v.

NEIMAN MARCUS GROUP LLC, and SNOWFLAKE, INC.,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* NEIMAN MARCUS GROUP LLC,
Registered Agent Name: Corporation Service Company
1200 South Pine Island Road
Plantation, Florida 32301

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Shamis & Gentile, P.A.
Andrew Shamis, Esq.
14 NE 1st Ave., Suite 705
Miami, FL 33132
Telephone: 305-479-2299

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

MARC REICHBART, individually and on behalf of all others similar situated,

Plaintiff(s)

v.

NEIMAN MARCUS GROUP LLC, and SNOWFLAKE, INC.,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* SNOWFLAKE, INC.,
Registered Agent Name: Corporation Service Company
1201 Hays Street
Tallahassee, Florida 32301

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Shamis & Gentile, P.A.
Andrew Shamis, Esq.
14 NE 1st Ave., Suite 705
Miami, FL 33132
Telephone: 305-479-2299

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset