IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

JAMILLAH SHERMAN, individually and on behalf of all others similarly situated, Plaintiffs, v. THE NEIMAN MARCUS GROUP LLC Defendant.	Case No.: **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

PLAINTIFFS' CLASS ACTION COMPLAINT

Plaintiff, Jamillah Sherman ("Plaintiff"), individually and on behalf of the Class defined below of similarly situated persons, allege the following against The Neiman Marcus Group LLC ("Neiman" or "Defendant") based upon personal knowledge with respect to Plaintiff's own experience, and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

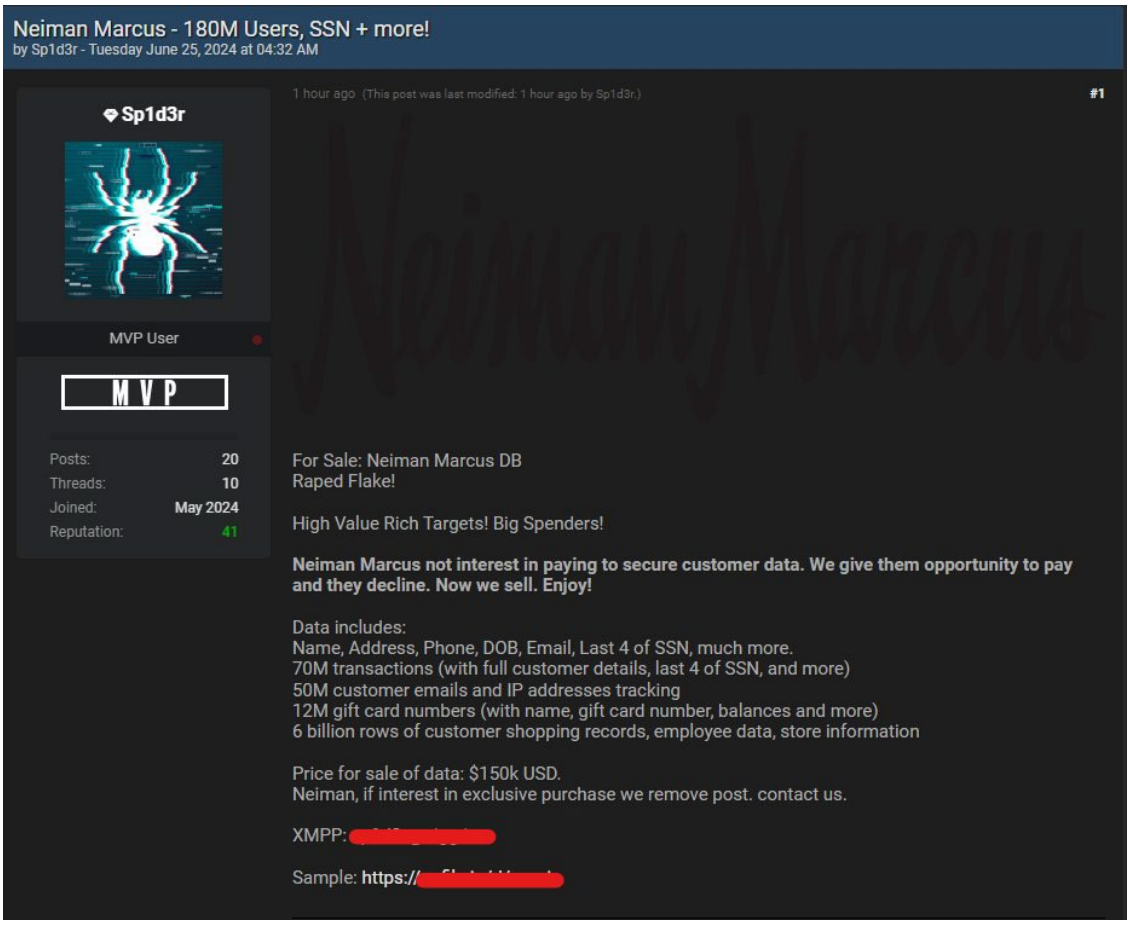
1. For all of the pomp and circumstance surrounding the premium brands and high-end fashion on its racks and shelves, luxury retailer Neiman Marcus takes a comparatively cut-rate approach to the data security protocols for its customers' data. While the rest of the civilized world utilizes multi-factor authentication and other modern security protocols to secure its data, Neiman Marcus still relies upon dangerously insecure "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 in the

crosshairs of hackers who now have access to their private personal and financial information. This action follows.

2. Plaintiff brings this class action case against Defendant The Neiman Marcus Group LLC for its failure to secure and safeguard customers' credit and debit card numbers and other payment card data ("PCD"), and other personally identifiable information ("PII") of customers and even employees, including names, emails, addresses, phone numbers, dates of birth, partial Social Security numbers, credit card numbers, transaction data, and employee identification numbers, and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class members that their PCD and PII (hereinafter, collectively, "Customer Data") had been stolen and precisely what types of information were stolen.

3. On or around May 24, 2024, it was discovered that during April and May of 2024, the personal information of Plaintiff and Class Members, which they had entrusted to Defendant with the expectation that it would be safeguarded against unauthorized access, was compromised in a data breach (hereafter referred to as the "Data Breach"). An hacker known as "Sp1d3r" claimed responsibility for the breach, asserting on June 25, 2024 in an online forum that Neiman Marcus declined to pay a ransom to recover its consumer data and offered it up for sale for $150,000.[1] According to the post, the Data Breach involved data for 70M transactions, 50M customer emails and IP addressed, 12M gift card numbers with balances, and 6 billion rows of customer shopping records, employee data, and store information:

[1] *See* https://x.com/H4ckManac/status/1805480891134697655 (last accessed 8/20/24)



4. Defendant could have prevented this Data Breach. Data breaches are a known threat, and technologies have emerged to protect consumer data housed for companies' benefit, such as two-factor authentication. While many retailers and other companies have responded to recent breaches by adopting technology that helps make data more secure, Defendant did not, instead relying upon outdated, antiquated security protocols.

5. This private Customer Data was compromised due to Defendant's acts and omissions and its failure to properly protect the Customer Data and was the inevitable result of Defendant's inadequate approach to data security and the protection of the Customer Data that it collected during the course of its business.

6. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard Customer Data, failing to take available steps to prevent and stop the Data Breach from ever happening, and failing to advise consumers of the Data Breach on a timely basis.

7. As a result of the Defendant's Data Breach, the Customer Data of Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members as a direct result of the Data Breach include the theft of their personal and financial information leading to: (1) the immediate need to take steps to protect their identity and finances, including closing accounts, alerting their banks, and monitoring their accounts and credit profiles; (2) unauthorized charges on their debit and credit card accounts; (3) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; (4) damages arising from the inability to use their debit or credit card accounts because their accounts needed to be closed, were suspended or otherwise rendered unusable as a result of the Data Breach, including but not limited to foregoing cash back rewards or points; (5) costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach; and, (6) other presently existing and/or imminent injury flowing from

potential fraud and identify theft posed by their Customer Data being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet black market.

8. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for Customer Data.

9. Further, Plaintiff and the Class retain a significant interest in ensuring that their Customer Data is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose Customer Data was stolen as a result of the Data Breach.

10. Plaintiff, on her own behalf and on behalf of all similarly situated consumers, seek to recover damages, and equitable and injunctive relief to prevent a reoccurrence of the Data Breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members, and, at least some members of the proposed Class have a different citizenship from Defendant.

12. This Court has jurisdiction over Defendant is incorporated in this District, with its registered agent located at 1209 Orange St, Wilmington, Delaware 19801.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is

incorporated in this District and thus resides here for venue purposes.

PARTIES

14. Plaintiff Jamillah Sherman is a resident and citizen of the State of New Jersey. She resided in North Carolina when she was a customer of Defendant Neiman Marcus and shared her customer data with it, and at the time of the Data Breach that is the subject of this litigation.

15. Plaintiff's Customer Data was entrusted to Defendant but was compromised in the Data Breach that is the subject of this litigation, exposing her private personal and financial information to criminals, and causing her damage as set forth in more detail herein.

16. Defendant The Neiman Marcus Group LLC is a Limited Liability Company organized under the laws of the State of Delaware. Defendant is a luxury retail store, noting on its website that, "Originally established in 1907, Neiman Marcus Group is a leader in luxury retail incorporating the internationally recognized names of several high-end brands. With its corporate headquarters in Dallas, Texas, NMG includes 36 brick-and-mortar stores of Neiman Marcus; 2 Bergdorf Goodman establishments; and 5 Last Call shops."[2] Defendant's registered agent for the service of process is located at 1209 Orange St, Wilmington, Delaware 19801.

STATEMENT OF FACTS

A. Consumer Plaintiff's Transactions

28. Plaintiff Jamillah Sherman has been a long-time customer of Neiman Marcus of over two decades. She has been a particularly frequent shopper over the previous 5 years, making weekly purchases at Neiman Marcus, both at brick-and-mortar locations and online. Purchases were made using her personal credit cards and debit cards to do so.

[2] *See* https://www.neimanmarcusgroup.com/our-brands (last visited 8/16/24)

29. Plaintiff is also a member of Defendant's loyalty program, and provided certain personal information to Defendant in connection with her registration and use of that program.

30. In late May of 2024, she received a notification indicating that her personal data had been found on the dark web. Since that time, she has had several anomalies on her credit profile, phishing attacks, and targeted hacking efforts directed to her financial accounts that she has had to address.

B. Neiman Marcus and Its Customer Data Collection Practices

17. Defendant operates luxury retail shopping establishments. When customers pay using credit or debit cards, Defendant collects Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. Defendant also collects other Customer Data in connection with gift cards, store credit cards, its customer loyalty program, and other transactions. Defendant stores the Customer Data off-site in the cloud using the third-party vendor, Snowflake.

18. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Customer Data collected, maintained and stored on its behalf is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

19. It is well known and the subject of many media reports that Customer Data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches at retailers, Defendant maintained an insufficient and inadequate system to protect the Customer Data of Consumer Plaintiff and Class members.

20. Customer Data is a valuable commodity because it contains not only payment card

numbers but PII as well. A black market exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on multiple underground Internet websites. Customer Data is valuable to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

21. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

22. Defendant was, or should have been, fully aware of the significant volume of daily credit and debit card transactions at its establishments, amounting to thousands of daily payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

23. Unfortunately, and as alleged below, despite all of this publicly available information and Defendant's knowledge of the continued compromises of Customer Data in the hands of other third parties, Defendant's approach to maintaining the privacy and security of the Customer Data of Plaintiff and Class members was lackadaisical, cavalier, reckless, and at the very least, negligent.

C. Neiman Marcus Failed to Comply with Industry Standards

24. Multi-factor authentication (MFA) has become the industry standard for protecting systems from unauthorized access due to its superior security capabilities compared to traditional single-factor authentication methods.

25. MFA is a security method that requires users to provide two or more verification factors to gain access to a resource such as a database, online account, or other digital platform. It is designed to enhance security beyond the traditional username and password combination by adding extra layers of protection against unauthorized access.

26. Traditional single-factor authentication using only a username and password is highly susceptible to various attack vectors. Brute-force attacks, where attackers systematically attempt numerous password combinations, can often crack weak or common passwords. Additionally, phishing attacks and credential stuffing, where attackers use stolen credentials from one service to access others, pose significant risks to systems protected only by passwords. These vulnerabilities are exacerbated by poor password hygiene, such as password reuse across multiple accounts or the use of easily guessable passwords.

27. Furthermore, the increasing sophistication of cyber threats has rendered traditional password-based authentication insufficient. Malicious actors can exploit flaws in authentication logic, compromise user credentials through data breaches, or employ social engineering tactics to bypass this basic security measure. The prevalence of stolen username and password combinations available on the dark web further underscores the inadequacy of relying solely on this method.

28. Using MFA, the user typically begins by entering a username and password as the first authentication factor. After successful verification of the first factor, the system prompts for an additional form of authentication. This could be a one-time password (OTP) sent via email, SMS, or generated by a mobile app, a biometric factor like a fingerprint or facial recognition scan, a physical token or security key, or answers to personal security questions.

29. By requiring multiple forms of verification, MFA significantly reduces the risk of

unauthorized access, even if one factor (like a password) is compromised. This makes it a crucial component of modern cybersecurity strategies for both organizations and individuals, and the baseline industry standard for data security. In contrast, the reliance on a simple username and password combination for authentication falls significantly below the current standard of care in cybersecurity due to several critical vulnerabilities and the evolving threat landscape.

30. Industry standards and best practices now require the implementation of multi-factor authentication (MFA) as a crucial component of a robust cybersecurity strategy that has been widely adopted across various industries, including finance, healthcare, and technology. Leading security organizations, such as the National Institute of Standards and Technology (NIST)[3] and the Cybersecurity and Infrastructure Security Agency (CISA),[4] strongly recommend the use of MFA as a critical component of a robust cybersecurity strategy.

31. This evolution in security practices is a direct response to the increasing sophistication of cyber threats and the inadequacy of simple username and password combinations in safeguarding sensitive information and systems.

32. The widespread adoption of MFA as an industry standard, coupled with its proven effectiveness in enhancing security, establishes a clear benchmark for reasonable care in protecting systems from unauthorized access. The continued reliance on simple username and password authentication falls short of this standard and exposes organizations and their users to significant

[3] *See* https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf (last accessed 8/20/24)

[4] *See* https://www.cisa.gov/MFA (last accessed 8/20/24)

and unnecessary risks in today's complex cybersecurity landscape.

33. Accordingly, the standard of care in the industry required Defendant to insist upon the implementation of MFA to properly secure and protect Consumer Data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt Customer Data that needs to be stored for any period of time.

34. Despite its awareness of its data security obligations, Defendant's treatment of PCD and PII entrusted to it by its customers fell far short of satisfying its legal duties and obligations. Neiman Marcus failed to ensure that access to its data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

D. Defendant Failed to Comply With FTC Requirements

35. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[5]

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

[5] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited 8/16/24).

practices for business.[6] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

37. The FTC recommends that companies not maintain cardholder 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.[7]

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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.

39. Defendant's failure to employ reasonable and appropriate measures to protect

[6]Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited 8/16/24).
[7] *Supra* n.5.

against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

40. In this case, Defendant was at all times fully aware of its obligation to protect its customers' financial and personal data because of its participation in payment card processing networks. Defendant was also aware of the significant repercussions if it failed to do so because it collected payment card data from thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

41. Despite understanding the consequences of inadequate data security, Defendant failed to implement MFA that would have protected its customers' data, and otherwise failed to take other measures necessary to protect its customer data.

E. The Data Breach

42. Defendant understands the importance of protecting personal information – the "Security" section of its privacy policy begins by affirming that:

> 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 and compliance best practices.[8]

43. Neiman Marcus failed to live up to its own standards. Starting on or about April 14, 2024, hackers began accessing Customer Data stored at Defendant's behest on Snowflake's servers. This was discovered on May 24, 2024.[9]

---

[8] *See* https://assistance.neimanmarcus.com/privacy?itemId=cat33940739#securityandprivacy (last visited 8/20/24)

[9] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/f5f736b6-9f8e-4d3f-9d24-d5d14ab9d56f.html (last accessed 8/20/24)

44. The breach became public on June 24, 2024, when Defendant began notifying customers.[10]

45. At the same time, Defendant notified the Attorney General for the State of Maine, asserting at that time that only 64,472 people were impacted by the Data Breach.[11]

46. Defendant's representation to the Attorney General was wrong, and in fact understated the impact of the breach by millions. According to Troy Hunt, founder of HaveIBeenPwned?, a service that notifies people when their email addresses are leaked in a data breach, the breach actually exposed 31 million customer email addresses to criminals after analyzing the stolen data.[12]

47. The Customer Data was compromised due to Defendant's acts and omissions and its failure to properly protect the Customer Data, despite the fact Neiman Marcus should have been aware of recent data breaches impacting other national retailers who only implemented single-factor authentication to protect its data.

48. In addition to Defendant's failure to prevent the Data Breach, Neiman Marcus also failed to detect the breach for over a month and then underreported – and thus under-notified consumers – the breadth and impact of the Data Breach.

49. The Data Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting Customer Data.

F. The Neiman Marcus Data Breach Caused Harm and Will Result in Additional Fraud

[10] https://www.maine.gov/cgi-bin/agviewerad/ret?loc=654 (last accessed 8/20/24)
[11] *Supra* n.9.
[12] https://www.techradar.com/pro/security/neiman-marcus-data-breach-exposed-millions-of-user-email-addresses (last accessed 8/20/24)

50. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, they can steal your identity, drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance.[13]

51. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. An October 2023 report of the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims reported spending an average of about 7 hours resolving the consequences of fraud in 2021.[14]

52. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

53. Thus, Plaintiff and Class members now face years of constant surveillance of their Customer Data, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the

---

[13] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited 8/20/24).
[14] Victims of Identity Theft, 2021 (Oct. 2023) available at: https://bjs.ojp.gov/document/vit21.pdf (last visited 8/20/24).
[15] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited 8/20/24).

resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

G. Plaintiff and Class Members Suffered Damages

54. The Customer Data of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Defendant. Defendant did not obtain Plaintiff's and Class members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

55. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

56. Neiman Marcus had the resources and technology available to prevent a breach. Upon information and belief, its data storage partner, Snowflake, offered MFA as an option to safeguard the Class Member's Customer Data held at Defendant's behest. Defendant, however, declined the use of MFA and instead opted to rely upon outdated, antiquated, and insecure single-factor authentication to secure this data.

57. Defendant neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

58. Had Defendant remedied the deficiencies in its security protocols and adopted

security measures recommended by experts in the field, Defendant would have prevented intrusion into its systems and, ultimately, the theft of its customers' confidential information.

59. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

60. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed

in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet card black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their Customer Data;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

61. While the Customer Data of Plaintiff and members of the Class has been stolen, Defendant continues to hold Customer Data of consumers, including Plaintiff and Class members. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and members of the Class have an undeniable interest in insuring that their Customer Data is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

62. Plaintiff seeks relief on behalf of Plaintiff's self and as a representative of all others who are similarly situated. Pursuant to Rule 23(a), (b)(2), (b)(3) and (c)(4), Fed. R. Civ. P., Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons residing in the United States who made a credit or debit card purchase with any affected Neiman Marcus Group business during the period of the Data Breach (the "Nationwide Class").

63. Excluded from each of the above Classes are Defendant and any of its affiliates, parents or subsidiaries; all officers and directors of Defendant; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

64. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

65. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

66. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is

impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class is believed to include millions of customers whose data was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

67. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Defendant had a duty to protect Customer Data;

b. Whether Defendant knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Defendant's security measures to protect their systems were reasonable in light of the current industry standards, FTC data security recommendations, and best practices recommended by data security experts;

d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendant's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Customer Data of Plaintiff and Class members;

g. Whether Plaintiff and Class members were injured and suffered damages or other acceptable losses because of Defendant's failure to reasonably protect its data systems and data network; and,

h. Whether Plaintiff and Class members are entitled to relief.

68. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a consumer who made purchases with one of Defendant's business entities, thus shared her data, and had that data compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

69. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Consumer Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

70. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual

litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

71. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

72. Likewise, particular issues under Rule 23(c)(4) 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 public of the Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Customer Data;

c. Whether Defendant's security measures to protect its systems were reasonable in light of industry standards, FTC data security recommendations, and other best practices recommended by data security experts;

d. Whether Defendant's failure to adequately comply with industry standards and/or to institute protective measures beyond those standards amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the Customer Data of Plaintiff and the Class members; and,

f. Whether adherence to industry standards, FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

73. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to information regarding which of its customers were affected by the Data Breach, the time period of the Data Breach, and which customers were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

74. Plaintiff restates and realleges the preceding paragraphs as if fully set forth herein.

75. Defendant solicited and invited Plaintiff and Class members to shop at their locations and make purchases using their credit or debit cards as form of payment. Plaintiff and Class members accepted Defendant's offers and used their credit or debit cards to make purchases at Defendant's stores during or prior to the period of the Data Breach.

76. When Consumer Plaintiff and Class members purchased and paid for Defendant's products using payment cards, they provided their Customer Data, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip and chip of, their debit and credit cards. In so doing, Plaintiff and Class members entered into mutually agreed-upon implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect

such information and to timely and accurately notify Plaintiff and Class members if their data had been breached and compromised.

77. Plaintiff and Class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic stripes of their credit and debit cards, to Defendant to shop and make purchases in the absence of the implied contract between them and Defendant.

78. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

79. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the PII and PCD of Consumer Plaintiff and Class members and by failing to provide timely and accurate notice to them that their Customer Data was compromised as a result of the Data Breach.

80. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant and Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

COUNT II
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

81. Plaintiff restates and realleges the preceding paragraphs as if fully set forth herein.

82. Upon accepting and storing the Customer Data of Plaintiff and Class members in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Customer Data was private

and confidential and should be protected as private and confidential.

83. Defendant owed a duty of care not to subject Plaintiff and Class members, along with their Customer Data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

84. Defendant owed numerous duties to Plaintiff and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Customer Data in its possession;

b. to protect Customer Data using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

85. Defendant also breached its duty to Plaintiff and the Class members to adequately protect and safeguard Customer Data by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Customer Data. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Customer Data with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Customer Data of Plaintiff and Class members, misuse the Customer Data and intentionally disclose it to others without consent.

86. Defendant knew, or should have known, of the risks inherent in collecting and storing Customer Data, the vulnerabilities of its systems, and the importance of adequate security.

Defendant knew about numerous, well-publicized data breaches within the retail industry.

87. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Customer Data.

88. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Customer Data of Plaintiff and Class members.

89. Because Defendant knew that a breach of its systems would damage hundreds of thousands, if not millions, of Defendant's customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Customer Data contained thereon.

90. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Defendant with their Customer Data was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the Customer Data it stored on them from attack.

91. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Customer Data. Defendant's misconduct included failing to: (1) secure its data systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

92. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' Customer Data and promptly notify them about the Data Breach.

93. Defendant breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Customer Data of Plaintiff and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' Customer Data both before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' Customer Data had been improperly acquired or accessed.

94. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Customer Data of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Customer Data of Plaintiff and Class members during the time it was within Defendant's possession or control.

95. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Customer Data to Plaintiff and the Class so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Customer Data.

96. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting to notify Plaintiff and Class members and then by failing to provide Plaintiff and Class members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Plaintiff and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

97. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Customer Data of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Customer Data of Plaintiff and Class members during the time it was within Defendant's possession or control.

98. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

99. Upon information and belief, Defendant improperly and inadequately safeguarded Customer Data of Plaintiff and Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect sensitive Customer Data of Plaintiff and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Customer Data of Plaintiff and Class members.

100. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Customer Data;

failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Customer Data of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive Customer Data had been compromised.

101. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Customer Data as described in this Complaint.

102. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Plaintiff and Class members; damages arising from Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

103. Plaintiff restates and realleges the preceding paragraphs as if fully set forth herein.

104. 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 Customer Data. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

105. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored, and the foreseeable consequences of a data breach at a chain as large as Defendant, including, specifically, the immense damages that would result to Plaintiff and Class members.

106. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

107. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

108. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

109. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiff's inability to use

their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT IV
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

110. Plaintiff restates and realleges the preceding paragraphs as if fully set forth here.

111. Plaintiff and Class members gave Defendants their Consumer Data in confidence, believing that Defendant would protect that information. Plaintiff and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant'' acceptance and storage of Plaintiffs' and Class members' Consumer Data created a fiduciary relationship between Defendant and Plaintiffs and Class members. In light of this relationship, Defendant must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff and Class Members' Consumer Data.

112. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff and Class Members' Consumer Data, failing

to comply with Section 5 of the FTCA, and otherwise failing to safeguard Plaintiff and Class members' Consumer Data that it collected.

113. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their Consumer Data; (iv) breach of the confidentiality of their Consumer Data; (v) deprivation of the value of their Consumer Data, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

114. Plaintiff restates and realleges the preceding paragraphs as if fully set forth here.

115. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their payment information. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their Customer Data with adequate data security.

116. Defendant knew that Plaintiff and Class members conferred a benefit on Defendant and accepted and has accepted or retained that benefit. Defendant profited from the purchases and used the Customer Data of Plaintiff and Class members for business purposes.

117. Defendant failed to secure the Customer Data of Plaintiff and Class members and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

118. Defendant acquired the Customer Data through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

119. If Plaintiff and Class members knew that Defendant would not secure their Customer Data using adequate security, they would not have made purchases at Defendant's stores.

120. Plaintiff and Class members have no adequate remedy at law.

121. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

122. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

123. Plaintiff restates and realleges the preceding paragraphs as if fully set forth here.

124. As previously alleged, Plaintiff and Class members entered into an implied contract that required Defendant to provide adequate security for the Customer Data it collected from their payment card transactions. As previously alleged, Defendant owes duties of care to Plaintiff and Class members that require it to adequately secure Customer Data.

125. Defendant still possesses Customer Data pertaining to Plaintiff and Class members.

126. Defendant has made no announcement or notification that it has remedied the

vulnerabilities in its computer data systems.

127. Accordingly, Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Defendant's lax approach towards data security has become public, the Customer Data in its possession is more vulnerable than previously.

128. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

129. Plaintiff, therefore, seeks a declaration that (a) Defendant's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access

to other portions of Defendant systems;

e. purging, deleting, and destroying in a reasonable secure manner Customer Data not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendant customers must take to protect themselves.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and their Counsel to represent the Nationwide Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Customer Data, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to consumer data collection, storage and

protection and to disclose with specificity to Class members the type of Customer Data compromised;

d. For an award of damages, including nominal damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: August 20, 2024

By: /s/ Scott M. Tucker

Scott M. Tucker (Del. Bar No. 4925)
Robert J. Kriner, Jr. (Del. Bar No. 2546)
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
2711 Centerville Rd., Suite 201
Wilmington, DE 19808
Tel.: 302-656-2500
smt@chimicles.com
rjk@chimicles.com

Steven A. Schwartz *(pro hac vice forthcoming)*
Beena M. McDonald *(pro hac vice forthcoming)*
Alex M. Kashurba*(pro hac vice forthcoming)*
Marissa N. Pembroke*(pro hac vice forthcoming)*
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

steveschwartz@chimicles.com
bmm@chimicles.com
amk@chimicles.com
mnp@chimicles.com

James J. Rosemergy *(pro hac vice forthcoming)*
CAREY, DANIS & LOWE
8235 Forsyth, Suite 1100
St. Louis, MO 63105
Tele: 314-725-7700
Direct: 314-678-1064
Fax: 314-721-0905
jrosemergy@careydanis.com

Attorneys For Plaintiff and The Proposed Class

JS 44 (Rev. 09/19)

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

Jamillah Sherman

(b) County of Residence of First Listed Plaintiff Essex, NJ
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Robert J. Kriner, Jr. and Scott M. Tucker
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
2711 Centerville Rd., Suite 201. Wilmington, DE 19808 - 302-656-2500

DEFENDANTS

The Neiman Marcus Group LLC

County of Residence of First Listed Defendant New Castle, DE
(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	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	**PERSONAL INJURY**	**PERSONAL INJURY**	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		**PROPERTY RIGHTS**	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	**PERSONAL PROPERTY**	**LABOR**	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	**SOCIAL SECURITY**	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit (15 USC 1681 or 1692)
❒ 190 Other Contract	☒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 485 Telephone Consumer Protection Act
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 490 Cable/Sat TV
❒ 196 Franchise				❒ 864 SSID Title XVI	❒ 850 Securities/Commodities/ Exchange
				❒ 865 RSI (405(g))	❒ 890 Other Statutory Actions
REAL PROPERTY	**CIVIL RIGHTS**	**PRISONER PETITIONS**		**FEDERAL TAX SUITS**	❒ 891 Agricultural Acts
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	**Habeas Corpus:**		❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 893 Environmental Matters
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee		❒ 871 IRS—Third Party 26 USC 7609	❒ 895 Freedom of Information Act
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			❒ 896 Arbitration
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty	**IMMIGRATION**		❒ 950 Constitutionality of State Statutes
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	**Other:**	❒ 462 Naturalization Application		
	❒ 448 Education	❒ 540 Mandamus & Other	❒ 465 Other Immigration Actions		
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

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(d)(2)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,001,000.00

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 08/20/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Scott M. Tucker

FOR OFFICE USE ONLY

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