John Heenan
Joseph Cook
HEENAN & COOK
1631 Zimmerman Trail
Billings, Montana 59102
Tel: (406) 839-9091
john@lawmontana.com
joe@lawmontana.com

Lesley E. Weaver*
BLEICHMAR FONTI & AULD LLP
1330 Broadway, Suite 630
Oakland, California 94612
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com

Counsel for Plaintiff Natalie Gianne and the Proposed Class

Additional counsel appear on signature page

** Pro Hac Vice application forthcoming*

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BUTTE DIVISION

NATALIE GIANNE, individually, and on behalf of all others similarly situated, Plaintiff, v. THE NEIMAN MARCUS GROUP LLC and SNOWFLAKE, INC., Defendant.	Case No. CV-24-102-BU-BMM **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Natalie Gianne, individually and on behalf of all others similarly situated, brings this class action against The Neiman Marcus Group LLC and Snowflake, Inc. (collectively, "Defendants"), and alleges, upon personal knowledge as to her own actions, and upon information and belief as to her counsel's investigation and as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this proposed class action against Defendants for their failure to safeguard the sensitive information of their customers from a foreseeable cyberattack. Plaintiff's personally identifiable information ("PII") was compromised as a result of the breach of The Neiman Marcus Group LLC's cloud-based data records stored with and entrusted to Snowflake.

2. The Neiman Marcus Group LLC ("Neiman Marcus") is the parent company of American luxury department store chains Neiman Marcus and Bergdorf Goodman. Neiman Marcus focuses on luxury clothing brands and designer goods.

3. Snowflake, Inc. ("Snowflake") is a large cloud-based data warehouse platform that provides businesses with "a single platform to access all data, including data that's unstructured, in open formats, and from third-parties."[1] Snowflake's over 9,000 clients include defendant Neiman Marcus, AT&T, Adobe, Kraft Heinz, Mastercard, Micron, Capital One, DoorDash, HP, Nielsen, Novartis, Okta, PepsiCo,

[1] https://www.snowflake.com/en/why-snowflake/ (last visited September 20, 2024).

Siemens, Instacart, JetBlue, NBCUniversal, US Foods, Western Union, Yamaha, and many others.

4. Snowflake promotes itself as a leader in the data security industry that "was built to deliver end-to-end data security for all users."[2] It purportedly "follows world-class, standards-based practices for the controls and processes that secure it and is based on a multilayered security architecture to protect customer data and access to that data."[3] Snowflake states that "[a]ll aspects of [its] architecture, implementation, and operation are designed to protect customer data in transit and at rest against both current and evolving security threats."[4]

5. Notwithstanding its proclaimed first-in-class data security standards, on May 23, 2024, Snowflake became aware that an unauthorized third party had gained access to Snowflake's platform and accessed numerous of its clients' accounts (the "Data Breach"). The third-party threat actor, tracked as UNC5537, claimed to have accessed employee and customer data for 165 of Snowflake's clients, including Neiman Marcus, AT&T, Advanced Auto Parts, LendingTree's subsidiary QuoteWizard, Ticketmaster, and Santander Bank.

---

[2] *Intro to Data Security*, SNOWFLAKE, https://www.snowflake.com/trending/intro-to-data-security (last visited September 20, 2024).
[3] *Id.*
[4] *Id*.

6. Subsequently, many of Snowflake's clients revealed that the data they had stored on Snowflake's platform had been exfiltrated in the Data Breach.

7. In June 2024, Neiman Marcus began notifying its customers that it had used a cloud-based data platform and that an "unauthorized third party obtained certain personal information stored in the database platform."[5] The information accessed in this data breach included both employee and customer information, including names, email and postal addresses, phone numbers, dates of birth, gift card information, transaction data, partial credit card numbers, the last four digits of Social Security numbers, and employee identification numbers.[6]

8. Defendants' failure to implement standard security measures was a significant factor leading to the Data Breach. Snowflake did not automatically require its clients to use multifactor authentication ("MFA"), for instance, despite being well aware of the risks of cyberattack and data theft. In fact, a selling point of Snowflake's systems was that they were easy to use and clients did not need to set up additional security configurations.[7] In addition, upon information and belief, Neiman Marcus also did not implement MFA or other standard security measures on its Snowflake account.

---

[5] https://www.neimanmarcusgroup.com/nmg-data-security (last visited September 20, 2024).
[6] *Id.*
[7] https://www.snowflake.com/en/resources/learn/snowflake-security-hub/ (last visited September 20, 2024).

9. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard the sensitive and personally identifiable information of Plaintiff and other members of the proposed class ("Class Members") whose data was stored and maintained by Snowflake. As a direct and proximate result of Defendants' failure to implement and follow standard security measures, the value of Plaintiff's and Class Members' personal information diminished. Plaintiff and Class Members further face an increased risk of identity theft and fraud due to the Data Breach, and must also devote substantial time, money, and energy to protect themselves, to the extent possible from these crimes.

II. PARTIES

10. **Plaintiff Natalie Gianne** is a natural person, resident, and citizen of California. Plaintiff Gianne signed up for a Neiman Marcus store credit card in 2012, which she closed in or around 2019. Plaintiff Gianne shopped regularly at Neiman Marcus and belonged to Neiman Marcus' loyalty program. In order to obtain a Neiman Marcus credit card and to participate in the loyalty program, Plaintiff Gianne provided Neiman Marcus with her personal information. Upon information and belief, Plaintiff Gianne's information was stored and maintained on the cloud-based data platform operated by Snowflake. As a result of Defendants' failure to safeguard Plaintiff's personal information, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

11. On September 13, 2024, Plaintiff Gianne logged into her account on the website of Credit Karma, a data protection service she uses to monitor her personal information for identity theft, hacking, and other security issues. Plaintiff Gianne was informed by Credit Karma that her personal data had been stolen as part of the Data Breach and theft of Neiman Marcus data. Credit Karma offers free identity monitoring to educate consumers about data security and enable them to determine if their personal information has been exposed on the dark web. Credit Karma states that they will "tell you which data breaches have included your personal info, so you can take action immediately."[8] In order to determine whether an individual's personal data has been exposed, Credit Karma scans "billions of records from public data breaches and the dark web, [and] has created a tool that runs searches for the email address associated with your Credit Karma account to tell you if your information was a part of a data breach."[9]

12. As a result of Defendants' conduct, Plaintiff Gianne suffered significant harm, including diminution in the value of her personal information, an increased

[8] Credit Karma offers free identity monitoring to educate consumers about data security and enable them to determine if their personal information has been exposed on the dark web. Credit Karma states that they will "tell you which data breaches have included your personal info, so you can take action immediately." https://www.creditkarma.com/id-monitoring (last visited September 20, 2024).

[9] https://support.creditkarma.com/s/article/About-Identity-Monitoring-US?categfilter=Identity_Monitoring_US&childcateg=Identity%20Monitoring&articledetail=true (last visited September 20, 2024).

risk of identity theft and fraud, and lost time spent investigating the Breach and monitoring her accounts.

13. **Defendant The Neiman Marcus Group LLC** is a Delaware limited liability company with its principal place of business located at 1618 Main Street, Dallas, Texas 75201. Neiman Marcus operates thirty-six brick-and-mortar Neiman Marcus stores and two Bergdorf Goodman stores, as well as Horchow, a home accessories store. Since 2020, Neiman Marcus has been owned by a group of shareholders, including Pacific Investment Management Co., Davidson Kempner Capital Management LP and Sixth Street Partners LLC.[10] In July 2024, it was announced that Neiman Marcus would be acquired by HBC, the parent company of Saks Fifth Avenue, for $2.65 billion.[11]

14. **Defendant Snowflake, Inc.** is a Delaware corporation with its headquarters and principal place of business located at 106 East Babcock Street, Suite 3A, Bozeman, Montana 59715. Snowflake is a publicly traded corporation listed on the New York Stock Exchange with revenues totaling approximately $829 million for the three months ended on April 30, 2024.[12] Snowflake's Data Cloud

[10] https://www.wsj.com/articles/neiman-marcus-approved-to-exit-bankruptcy-after-critics-arrest-11599253848?mod=article_inline (last visited September 20, 2024).
[11] https://www.neimanmarcusgroup.com/HBC,-Parent-of-Saks-Fifth-Avenue,-to-Acquire-Neiman-Marcus-Group-for-2-65-Billion-and-Establish-Saks-Global,-a-Technology-Powered-Luxury-Retail-Company (last visited September 20, 2024).
[12] https://www.bamsec.com/filing/164014724000135?cik=1640147 (last visited September 20, 2024).

platform is used globally, with 9,822 institutions trusting Snowflake to manage and store customers' data.[13] The "substantial majority" of such revenue comes from fees charged to Snowflake's customers "based on the compute, storage, and data transfer resources consumed on [its] platform."[14]

III. JURISDICTION AND VENUE

15. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which one or more members of the proposed class, including Plaintiff, are citizens of a state different from Defendant. The Court has supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the same case or controversy.

16. This Court has personal jurisdiction over Snowflake because Snowflake's headquarters and principal place of business is located in Bozeman, Montana.

[13] *Id.*
[14] *Id.*

IV. FACTUAL ALLEGATIONS

A. Defendants Represented That They Would Keep Customers' Data Safe and Secure

17. Snowflake is a cloud-based platform that provides "digital warehouse" storage and analytics services to over 9,000 clients, which are generally businesses and companies such as AT&T, Capital One, NBCUniversal, and Ticketmaster, among many others. Snowflake states on its website that "everything is easier in the AI data cloud."[15] It promises that by eliminating data silos and simplifying architecture through the use of Snowflake, the user "can get more value from your data." Snowflake encourages companies to take advantage of the "near-infinite scale" of its cloud storage: "Bring more workloads, users and use cases directly to your data."

18. In addition to the advantages of the "infinite storage" available in cloud-based data storage, Snowflake also highlights the cost-saving benefits of its services. Its fully managed cloud service can "automate costly and complex operations to reduce overheard [sic] and improve efficiency." Among the key elements of its platform described in its most recent Form 10-K, filed on March 26, 2024, Snowflake touted its "optimized price-performance": "Our platform uses advanced optimizations to efficiently access only the data required to deliver the desired

[15] https://www.snowflake.com/en/ (last visited September 20, 2024).

results. It delivers speed without the need for tuning or the expense of manually organizing data prior to use. Organizations can adjust their consumption to precisely match their needs, always optimizing for price-performance."

19. Snowflake frequently touted the cost-saving benefits of the cloud on its website, including in this case-study on the cost savings enjoyed by AT&T after using Snowflake's cloud-based data platform: [16]

> AT&T Provides Faster Insights While Lowering Estimated Annual Costs by 84%. This premier enterprise gives more teams near-instant access to powerful insights for better decision-making and customer experiences — all while cutting costs and improving performance by switching to Snowflake.
> KEY RESULTS: 84% Savings on estimated annual costs, thanks to results caching.

Among the highlights of the AT&T case-study, Snowflake identified the following:

- Proactive troubleshooting for a better customer experience: Democratized access to data helps AT&T find and fix issues—before they impact customers.
- Greater collaboration, fewer silos: Snowflake's Secure Data Sharing eliminates internal silos and allows AT&T's business

[16] https://www.snowflake.com/en/customers/all-customers/case-study/att/ (last visited September 20, 2024).

partners to maintain control of their data while sharing—without having to move or copy data.

20. Snowflake markets itself as a leader in the data security industry, claiming to "set the standard for data security." It claims it "was built to deliver end-to-end data security for all users," "world-class, standards-based practices for the controls and processes . . . to protect customer data and access to that data," and "comprehensive security framework."[17] It further claims that "[a]ll aspects of Snowflake's architecture, implementation, and operation are designed to protect customer data in transit and at rest against both current and evolving security threats."[18]

21. Snowflake further acknowledges the risk of data breaches and utilizes this threat to promote its products. Snowflake's website states, for instance:[19]

- "In today's connected world where cybercriminals have greater opportunity than ever before, data security is crucial for every business."

[17] *Intro to Data Security*, SNOWFLAKE, https://www.snowflake.com/trending/intro-to-data-security (last visited September 20, 2024).
[18] *Id.*
[19] *Id.*

- "Data breaches cause customers to lose trust in a business, and they can significantly damage a company's reputation if news of the breach gets out to the media."
- "[D]ata security should be a priority for every business in every industry, not just highly regulated industries such as healthcare and finance."

22. Snowflake has experienced great success and tremendous growth for the company as a result of its offering of cloud-based data warehousing services. It posted a revolving graphic identifying some of the more than 7,200 "leading companies [that] lead with Snowflake," including Zoom, Sub-Zero, Orangetheory Fitness, Adobe, Cisco, Comcast, and the University of Notre Dame, in addition to AT&T and other companies previously mentioned. In its latest Form 10-K, Snowflake noted that in the month of January alone, "we processed an average of approximately 4.2 billion daily queries across all our customer accounts, up from an average of approximately 2.6 billion daily queries during the corresponding month of the prior fiscal year." And as of January 31, 2024, Snowflake had 9,437 customers, up from 7,744 customers as of January 31, 2023. Snowflake's revenue similarly increased: "For the fiscal years ended January 31, 2024, 2023, and 2022, our revenue was $2.8 billion, $2.1 billion, and $1.2 billion, respectively, representing year-over-year growth of 36% and 69%, respectively."

23. Partly as a result of its representations, Snowflake's clients entrust it with large amounts of customer data.

24. Further, Defendant Neiman Marcus promised its customers that it would protect their data. Neiman Marcus' Privacy Policy states: "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."[20]

25. Neiman Marcus' Privacy Policy also explains that customer PII may be shared by Neiman Marcus with certain third parties, such as service providers, but they assured customers even those third parties would protect customers' personal data:

> We also may disclose information to outside companies that help us bring you the products and services we offer. For example, we may work with an outside company to: (a) manage a database of customer information; (b) assist us in distributing emails; (c) assist us with marketing and data collection; (d) provide us storage and analysis; (e) provide fraud prevention; and (f) provide other services designed to assist us in maximizing our business potential. We require that these outside companies agree to keep

[20] https://assistance.neimanmarcus.com/privacy#securityandprivacy (last visited September 20, 2024).

> confidential all information we share with them, use the information only to perform their obligations in our agreements with them, and abide by applicable data privacy laws.[21]

26. Neiman Marcus also acknowledged in its privacy policy that it had a duty to protect customer data, stating: "Neiman Marcus, One Marcus Square, 1618 Main Street, Dallas, Texas 75201 is responsible for your privacy protection."[22]

B. <u>Plaintiff's and Class Members' PII was Exposed in the Data Breach</u>

27. In April 2024, the cybersecurity firm, Mandiant, received information regarding a suspected theft of data from Snowflake's platform. Mandiant informed Snowflake and was engaged by Snowflake to investigate the suspected breach. Pursuant to that investigation, Mandiant determined that Snowflake's platform had been compromised by a threat actor "using credentials previously stolen via infostealer malware" and that the threat actor "used these stolen credentials to access the customer's Snowflake instance and ultimately exfiltrate valuable data."[23]

28. Mandiant further concluded that "the credentials were easily accessed by bad actors in part because impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password." While Snowflake made MFA available to its

---

[21] *Id.*
[22] *Id.*
[23] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion (last visited September 20, 2024).

customers, the use of MFA was not required to access customers' data and administrators could not set MFA policies systemwide.

29. Snowflake's security failure was compounded by Neiman Marcus' additional failure to encrypt or institute additional multi-factor authentication protections for its data stored by Snowflake.

30. Analysis also showed that some of the compromised Snowflake credentials had been for sale on the Dark Web for years and were still valid, which means those credentials hadn't been rotated or updated, as would be typically required in a secured system.[24] Further, Snowflake did not create or require its clients to create network allow lists, which is a list of sanctioned entities, such as IP addresses, domains, and applications, to control access to Snowflake's service or internal stage.[25]

31. Moreover, Snowflake did not provide proper guidance to its clients, such as Neiman Marcus, regarding setting secure configurations. In fact, a selling point of Snowflake's systems was the fact that it could be easily used by its clients without having to set up additional security configurations. Had Snowflake required these security configurations, the Data Breach may have been avoided.

---

[24] https://www.darkreading.com/threat-intelligence/snowflake-account-attacks-driven-by-exposed-legitimate-credentials (last visited September 20, 2024).

[25] https://docs.snowflake.com/en/user-guide/network-policies (last visited September 20, 2024).

32. On May 22, 2024, Mandiant began contacting Snowflake's clients to inform them of the breach. As of June 10, 2024, Mandiant and Snowflake had notified approximately 165 potentially exposed organizations. The organizations whose data were compromised as a result of this Breach include Neiman Marcus, AT&T, Advanced Auto Parts, LendingTree's subsidiary QuoteWizard, Ticketmaster operator Live Nation, and Santander Bank.

33. The stolen data includes the personal information of Neiman Marcus customers and employees, "and included information such as names, contact information (e.g., email and postal addresses, and phone numbers), dates of birth, Neiman Marcus and Bergdorf Goodman gift card information (without gift card PINs), transaction data, partial credit card numbers (without expiration dates or CVVs), the last four digits of Social Security numbers, and employee identification numbers."[26]

34. In a data breach notice, Neiman Marcus reported that it "promptly" took action to resolve the issue, including that it had disabled access to the database platform, engaged security experts, and coordinated with law enforcement.[27]

35. However, on June 25, 2024, the threat actor group, Sp1d3r, put the company's data up for sale on a dark web forum, asking for $150,000 in exchange

[26] https://www.neimanmarcusgroup.com/nmg-data-security (last visited September 20, 2024).
[27] *Id.*

for the stolen data set.[28] The third party group purported that the data set for sale consists of 70 million customer transactions complete with customer information, 50 million customer emails and IP addresses, and "6 billion rows of customer shopping records, store information, and employee data":[29]

For Sale: Neiman Marcus DB
Raped Flake!

High Value Rich Targets! Big Spenders!

Neiman Marcus not interest in paying to secure customer data. We give them opportunity to pay and they decline. Now we sell. Enjoy!

Data includes:
Name, Address, Phone, DOB, Email, Last 4 of SSN, much more.
70M transactions (with full customer details, last 4 of SSN, and more)
50M customer emails and IP addresses tracking
12M gift card numbers (with name, gift card number, balances and more)
6 billion rows of customer shopping records, employee data, store information

Price for sale of data: $150k USD.
Neiman, if interest in exclusive purchase we remove post. contact us.

XMPP: [redacted]

Sample: https://[redacted]

36. Subsequent reports confirm that over 30 million Neiman Marcus customers had their information exposed in the Data Breach.[30]

37. The information exposed as a result of the Data Breach is uniquely sensitive and includes PII and other personal data. Allowing cybercriminals to access this sensitive data leaves the customers of Snowflake's clients vulnerable to fraud

[28] https://www.techradar.com/pro/security/neiman-marcus-confirms-data-breach-claims-its-snowflake-account-was-hacked (last visited September 20, 2024).
[29] https://www.bleepingcomputer.com/news/security/neiman-marcus-data-breach-31-million-email-addresses-found-exposed/ (last visited September 20, 2024).
[30] https://www.bleepingcomputer.com/news/security/neiman-marcus-data-breach-31-million-email-addresses-found-exposed/ (last visited September 20, 2024).

and identity theft. Credit Karma, the credit and fraud alert service used by Plaintiff, notes that "Identity fraud can lead to significant financial consequences for victims. Fraudsters who have obtained your personal information can use your identity to open unauthorized accounts, take out loans, and more."[31]

38. Similarly, a CNN report on the incident identified several ways that bad actors can use stolen exposed customer data:

> [A] hacker could see that a customer is in constant contact with a big bank's line and could send a phishing attempt posing as the bank. The hacker could text the customer saying, "This is Bank of America. We have some suspicious activity on your account. Click this link to review the charges, or call this number," said John Dwyer, director of security research at Binary Defense, a cybersecurity solutions firm. Or the hacker could pose as someone the customer has a personal relationship with, like a friend or family member. The age of artificial intelligence makes this even more pressing, according to Collin Walke, cybersecurity and data privacy partner at Hall Estill. "Once they know who you've been communicating with, it allows deep fakes and those sorts of hacks to occur much easier," Walke said. Some customers' cell tower ID numbers were also exposed, which could help some bad actors track down geolocations, Walke said. That could also make these hacking attempts more believable.

39. Other Snowflake clients were similarly victimized by the Data Breach. For example, Live Nation, the parent company of Ticketmaster, acknowledged that

[31] https://support.creditkarma.com/s/article/About-Identity-Monitoring-US?categfilter=Identity_Monitoring_US&childcateg=Identity%20Monitoring&articledetail=true (last visited September 20, 2024).

data was stolen from its Snowflake account in May 2024.[32] Although Live Nation did not specify how much data had been accessed in the Data Breach, a known cybercrime organization, ShinyHunters, said it "had stolen user data of over 500 million Ticketmaster customers."[33] AT&T, another Snowflake client, has acknowledged that data for "nearly all" of the company's customers was exposed in the Snowflake breach, including customers' phone and text message records and other personal information.[34]

C. The Data Breach Was a Foreseeable Risk of Which Defendants Were on Notice and Could Have Prevented

40. Defendants had a responsibility to protect the personal information entrusted to it by Plaintiff and Class Members by implementing sufficient security measures, including but not limited to requiring its clients to institute MFA.

41. Defendants further had a duty to safeguard customers' PII pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "FTC Act"), which requires companies to maintain reasonable and appropriate data security measures. The FTC has issued guidance specifically to the entities which use cloud-based services, and reminded them that

[32] https://www.reuters.com/technology/cybersecurity/live-nation-probing-ticketmaster-hack-amid-user-data-leak-concerns-2024-06-01/ (last visited September 20, 2024).
[33] *Id.*
[34] https://www.nytimes.com/2024/07/12/business/att-data-breach.html (last visited September 20, 2024).

securing the information on the cloud-based services is their corporate responsibility.[35]

42. Defendant Snowflake is a sophisticated technology company—Snowflake is one of the largest cloud storage providers in the world. Snowflake is well aware of its duty to safeguard information and that the data it collects and stores are valuable targets for data thieves. Indeed, Snowflake identifies cyberattacks as a "risk factor" that could materially affect its business in its Form 10-K.[36]

43. Neiman Marcus also knew or should have known it was subject to attack. For example, in May 2021, Neiman Marcus commissioned an Audit Committee to examine, among other things, "cybersecurity risk and the steps management has taken to monitor and control such exposures."[37]

44. Yet, despite knowing that its clients' data was valuable and was at risk of cyberattack, Defendants continued to store massive amounts of its customers' data in an insecure manner.

45. Had Snowflake provided proper guidance to its clients for setting secure system configurations, such as requiring MFA to access customers' records

---

[35] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited September 20, 2024).

[36] https://www.sec.gov/ix?doc=/Archives/edgar/data/1640147/000164014724000101/snow-20240131.htm (last visited September 20, 2024).

[37] file:///C:/Users/JSamra/Downloads/Neiman%20Marcus%20Group%20-%20Audit%20Committee%20Charter%20(Appvd%20by%20Board%205-26-21).pdf (last visited September 20, 2024).

or setting network allow lists, the Data Breach may have been prevented. Rather than require these secure configurations, however, Snowflake marketed its systems as easy to use to its clients and did not properly monitor its clients' access.

46. Likewise, Neiman Marcus failed to encrypt or otherwise institute additional multi-factor authentication protections for the personal information of Plaintiff and Class Members stored by Snowflake.

47. Notably, since the Data Breach, Snowflake has established a new security policy to allow administrators to require MFA for all users or specific roles—further showing that this is a reasonable safety measure that Snowflake should have implemented pre-breach.[38]

48. Snowflake was aware of the importance of MFA as it is an industry standard that should be required "wherever possible."[39] Indeed, Snowflake identifies MFA as one of "8 Data Security Solutions" it recommended to combat "Common Data Security Risks" that render organizations vulnerable to data breaches:

> Network and security authentication: SSO, MFA. Network security provides the first line of defense. Federated single sign-on (SSO) establishes trusted relationships between separate organizations and third parties, such as partners, allowing them to share identities and authenticate users across domains. Multi-factor authentication (MFA) only allows access to a website or

[38] https://www.cybersecuritydive.com/news/snowflake-mfa-policy-change/720851/ (last visited September 20, 2024).

[39] https://www.cisa.gov/secure-our-world/require-multifactor-authentication (last visited September 20, 2024).

> application after the successful submission of two or more pieces of evidence to the authentication device.[40]

Despite understanding the importance of MFA, Snowflake inexplicably failed to implement it.

49. By failing to implement reasonable security measures to safeguard Plaintiff's and Class Members' PII, Defendants breached their duty to and disregarded the rights of Plaintiff and the Class Members.

D. <u>Injuries to Plaintiff and Class Members</u>

50. As a result of Defendants' inadequate security and breach of their duties and obligations, the personally identifiable information of Plaintiff and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiff and Class Members have suffered injuries as a direct and proximate result of Defendants' conduct. Plaintiff and Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

51. Plaintiff and other customers provided their sensitive data to Neiman Marcus, which paid Snowflake for its services. At least a partial payment for Snowflake's services was attributed to protecting Plaintiff's and Class Members' information in their possession, including the information released to criminals here.

[40] https://www.snowflake.com/trending/intro-to-data-security (last visited September 20, 2024).

52. Plaintiff and Class Members must now spend their own time, money, and energy to monitor their accounts to ensure personal information obtained in this Data Breach is not used to further harm them. This includes the need to review all financial activity, monitor credit status, update previously secure passwords and logins to an increasing variety of accounts, scrutinize communications, and seek out and purchase credit monitoring services and identity theft protection.

53. Once personal information is exposed, there is virtually no way to ensure that the exposed information has been recovered or contained against future misuse. In addition, there is the prospect that the stolen data can be aggregated and combined with the data from other data breaches.

V. CLASS ACTION ALLEGATIONS

54. Plaintiff brings this action on her own behalf, and on behalf of the following Classes:

The Nationwide Class

All individuals residing in the United States whose personally identifiable information was compromised as a result of the Data Breach.

The California Subclass

All individuals residing in California whose personally identifiable information was compromised as a result of the Data Breach

55. The Nationwide Class and Subclass is referred to herein as "Class," unless otherwise stated.

56. Excluded from the proposed Class are: Defendant, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

57. Plaintiff reserves the right to re-define the Class definition after conducting discovery.

58. **Numerosity (Fed. R. Civ. P. 23(a)(1)).** The Class Members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes millions of people whose PII was compromised as a result of the Data Breach. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

59. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3)).** Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to the following:

a. Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiff's and Class Members' PII;

b. Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiff's and Class Members' PII;

c. Whether Defendants acted willfully, recklessly, or negligently in connection with the maintenance of reasonable security procedures and practices to protect Plaintiff's and Class Members PII;

d. Whether Defendants' conduct, practices, actions, and omissions, resulted in or was the proximate cause of the Data Breach, resulting in the loss of Plaintiff's and Class Members' PII;

e. Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and Class Members;

f. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

g. Whether and when Defendants knew or should have known that their systems were vulnerable to attack;

h. Whether Defendants adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

i. Whether Defendants received a benefit without proper restitution making it unjust for Defendants to retain the benefit without commensurate compensation;

j. Whether Defendants violated state Unfair Competition Laws;

k. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their PII; and

l. Whether Plaintiff and Class Members are entitled to relief, including compensatory damaged, punitive damages, and/or statutory or civil penalties, and equitable relief.

60. **Typicality (Fed. R. Civ. P. 23(a)(3)).** Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the Class Members. Plaintiff's claims are typical of the claims of the members of the Class because all Class Members' reimbursement payments were delayed following the Data Breach and all Class Members were harmed as a result.

61. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)).** Pursuant to Rule 23(a)(4), Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Class Members. Plaintiff has retained counsel experienced in prosecuting class actions and data breach cases.

62. **Superiority (Fed. R. Civ. P. 23(b)(3)).** Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class Members because the amount of

monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

63. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

a. the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Class Members which would establish incompatible standards of conduct for Defendants; or

b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to individual Class Members which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

64. **Issue Certification (Fed. R. Civ. P. 23(c)(4)).** In the alternative, the common questions of fact and law, set forth in Paragraph 81, are appropriate for issue certification on behalf of the proposed Class.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class Against All Defendants)

65. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

66. Defendants owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in Defendants' possession, custody, or control.

67. Defendants knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and the importance of maintaining secure systems. Defendants knew, or should have known, of the vast uptick in data breaches in recent years. Defendants had a duty to protect the PII of Plaintiff and Class Members.

68. Given the nature of Defendants' business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Defendants had a duty to prevent.

69. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII.

70. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

71. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and the Class Members, their PII would not have been compromised.

72. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class Against All Defendants)

73. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

74. Defendants' duties arise from Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

75. Defendants violated Security Rules and Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and all other Class Members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

76. Defendants' violations of Security Rules and Section 5 of the FTCA constitute negligence *per se*.

77. Plaintiff and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

78. The harm occurring because of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

79. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

80. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violations of Security Rules and Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class Against All Defendants)

81. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

82. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for services—namely, they provided and entrusted Snowflake's customer, Neiman Marcus, with their valuable PII. Neiman Marcus, in turn, entrusted Plaintiff's and the Class Members' information to Snowflake, and on behalf of Plaintiff and the Class paid a fee to Snowflake for its data storage services. Therefore, Snowflake has been receiving payments (at least in

part) intended to protect Plaintiff's and Class Members' information. Neiman Marcus funds its data security measures (including to payments to Snowflake) from payments made by and on behalf of Plaintiff and the Class Members.

83. Neiman Marcus paid Snowflake (on behalf of Plaintiff and the Class) for its data storage services, a portion of which was intended to provide them with a reasonable level of data security from both Defendants in order to protect Plaintiff's and the Class Members' PII.

84. In exchange for their payment, Plaintiff and Class Members were entitled to reasonable measures to protect their PII.

85. Defendants appreciated, accepted, and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from their conduct toward Plaintiff and Class Members as described herein—namely, (a) Plaintiff and Class Members conferred a benefit on Defendants, and Defendants accepted or retained that benefit; and (b) Defendants used Plaintiff's and Class Members' PII for business purposes.

86. Defendants failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit provided on behalf of Plaintiff and Class Members.

87. Defendants acquired the PII through inequitable means in that it failed to disclose its inadequate security practices previously alleged.

88. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

89. Under the circumstances, it would be unjust and unfair for Defendants to be permitted to retain any of the benefits conferred by or on behalf of Plaintiff and the Class.

90. Under the principles of equity and good conscience, Defendants should not be permitted to retain the PII belonging to Plaintiff and Class Members because Defendants failed to implement the data management and security measures that industry standards mandate.

91. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received on behalf of and for the benefit of Plaintiff and the Class.

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant Snowflake)

92. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

93. Snowflake entered into contracts with its various corporate clients, including Neiman Marcus, to provide data storage services and maintain secure data cloud systems. These contracts were made expressly for the benefit of Plaintiff and

Class Members, who were customers and/or employees of Neiman Marcus. In order to effectuate offered services and upon information and belief as to the exact terms of the contract, Snowflake agreed to collect, store, and protect Plaintiff's and Class Members' PII.

94. Thus, the benefit of collection, protection, and storage of the PII was the direct, intended, and primary objective of the contracting parties.

95. Snowflake breached its contracts with its customers, including Neiman Marcus, when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

96. Snowflake knew that if it were to breach its contracts, the harm would befall its clients', including Neiman Marcus', customers and employees for whom the benefit was intended to confer. As such, Snowflake's failure to uphold the terms of its contracts and allow for the Data Breach has foreseeably harmed Plaintiff and the Class.

97. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with their costs including attorneys' fees incurred.

COUNT V
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class Against All Defendants)

98. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

99. Plaintiff and Class Members have a legally protected privacy interest in their PII that Defendants required them to provide and/or allow them to store.

100. Plaintiff and Class Members reasonably expected their PII would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

101. Defendants unlawfully invaded the privacy rights of Plaintiff and Class Members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) leaving their PII exposed to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) leaving their PII exposed to unauthorized parties without the informed and clear consent of Plaintiff and Class Members. This invasion into the privacy interest of Plaintiff and Class Members is serious and substantial.

102. In failing to adequately secure Plaintiff's and Class Members' PII, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class Members.

103. Defendants violated Plaintiff's and Class Members' right to privacy under the common law as well as under state and federal law.

104. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class Members' PII has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

COUNT VI
DECLARATORY RELIEF
(On Behalf of Plaintiff and the Class Against All Defendants)

105. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

106. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' duties to safeguard and protect Plaintiff's and Class Members' PII. Defendants' security measures were (and continue to be) woefully inadequate. Defendants dispute these contentions and contend that its security measures are appropriate.

107. Plaintiff and Class Members continue to suffer damages and exposure to other injury and harm, and without a declaratory relief, they will likely continue to suffer further injury, a possibility of a future data breach, and harm.

108. Therefore, Plaintiff and Class Members request a judicial determination of their rights and duties, and ask the Court to enter a judgment declaring, *inter alia*, (i) Defendants owed (and continue to owe) a legal duty to safeguard and protect Plaintiff's and Class Members' confidential and sensitive PII, and timely notify them about the Data Breach, (ii) Defendants breached (and continue to breach) such legal duties by failing to safeguard and protect Plaintiff's and Class Members' PII, and (iii) Defendants' breach of their legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiff and Class Members. A declaration from the Court ordering Defendants to stop their illegal practices is required. Plaintiff and Class Members will otherwise continue to suffer harm as alleged above.

1. CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT VII
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL"), CAL. BUS. & PROF. CODE §§ 1700, *et seq.*
(On Behalf of California Plaintiff and the California Subclass Against All Defendants)

109. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

110. Plaintiff Gianne (the "California Plaintiff") brings this Claim on behalf of herself and members of the California Subclass.

111. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

112. In the course of conducting its business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII, and by violating the statutory and common law alleged herein. Plaintiff and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

113. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends

legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45). The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

114. The UCL also prohibits any "fraudulent business act or practice." Defendants' above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

115. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying

expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages, (v) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

116. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself individually, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

COUNT VIII
VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT, CALIFORNIA CIVIL CODE §§ 1750, *et seq.*
(On Behalf of California Plaintiff and the California Subclass Against All Defendants)

117. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

118. Plaintiff Gianne (the "California Plaintiff") brings this Claim on behalf of herself and members of the California Subclass.

119. The California Consumer Legal Remedies Act ("CLRA") prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of goods.

120. Defendants' unlawful conduct described herein was intended to increase sales to the consuming public and violated and continue to violate Section 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the products and services have characteristics and benefits which they do not have.

121. Defendants fraudulently deceived California Plaintiff and the California Subclass by representing that its products and services have certain characteristics, benefits, and qualities which they do not have, namely data protection and security. In doing so, Defendants intentionally misrepresented and concealed material facts from California Plaintiff and the California Subclass, specifically by advertising secure technology when Defendants in fact failed to

institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving California Plaintiff and the California Subclass and depriving them of their legal rights and money.

122. Defendants' claims about the products and services led and continues to lead consumers like California Plaintiff to reasonably believe that Defendants have implemented adequate data security measures when Defendants in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access consumers' PII.

123. Defendants knew or should have known that adequate security measures were not in place and that consumers' PII was vulnerable to a data breach.

124. California Plaintiff and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendants' false representations.

125. California Plaintiff and the California Subclass would not have purchased the products or used the services, or would have paid significantly less for the products and services, had they known that their PII was vulnerable to a data breach.

126. Defendants' actions as described herein were done with conscious disregard of California Plaintiff's rights, and Defendants were wanton and malicious in their concealment of the same.

127. California Plaintiff and the California Subclass have suffered injury in fact and have lost money as a result of Defendants' unfair, unlawful, and fraudulent conduct. Specifically, California Plaintiff and the California Subclass paid for products and services advertised as secure, and consequentially entrusted Defendants with their PII, when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. California Plaintiff and the California Subclass would not have purchased the products and services or would not have provided Defendants with their PII, had they known that their PII was vulnerable to a data breach.

128. Defendants should be compelled to implement adequate security practices to protect consumers' PII. Additionally, California Plaintiff and the members of the California Subclass lost money as a result of Defendants' unlawful practices.

129. At this time, California Plaintiff and the California Subclass seek injunctive relief under the CLRA pursuant to Cal. Civ. Code § 1782(d); but they anticipate the need to amend the complaint and seek restitution.

COUNT IX
CALIFORNIA CONSUMER PRIVACY ACT,
CAL. CIV. CODE § 1798, *et seq.*
(On Behalf of California Plaintiff and the California Subclass Against All Defendants)

130. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

131. Plaintiff Gianne (the "California Plaintiff") brings this Claim on behalf of herself and members of the California Subclass.

132. The California Consumer Privacy Act ("CCPA") protects California consumers' constitutional right to privacy and provides consumers with a private right of action against businesses that breach their duty to take reasonable steps to protect consumers' personal information from unauthorized access, theft, or disclosure. Cal. Civ. Code § 1798.150(a)(1).

133. Defendants Neiman Marcus and Snowflake are each a "Business" as defined by the CCPA: a "legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information," and that both does business in the State of California and has "annual gross revenues in excess of twenty-five million dollars ($25,000,000)." Cal. Civ. Code § 1798.140(d).

134. California Plaintiff and the California Subclass are consumers as defined by the CCPA: "'Consumer' means a natural person who is a California resident." Cal. Civ. Code § 1798.140(i).

135. Defendants stored California Plaintiff's and the California Subclass' personal information, as defined by the CCPA: "'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1). Personal information can include but is not limited to: "Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers." Cal. Civ. Code § 1798.140(v)(1)(A).

136. Defendants collected, stored and/or transmitted California Plaintiff's and the California Subclass' personal information in a nonencrypted and nonredacted form. As a business under the CCPA, Defendants owed a duty to Plaintiff and the California Subclass "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Cal. Civ. Code § 1798.150(a)(1). California Plaintiff's personal information was accessed by third parties without authorization,

demonstrating that Defendants failed in their duty to implement and maintain reasonable security procedures and practices to protect California Plaintiff's personal information.

137. As a direct and proximate result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of California Plaintiff's personal information, California Plaintiff suffered unauthorized access and exfiltration, theft, or disclosure of her personal information.

138. As a direct and proximate result of the unauthorized disclosure of their personal information, California Plaintiff was injured and is at high risk of suffering further injury, including future data breaches, identity theft and fraud, and negative impact to her credit.

139. California Plaintiff seeks injunctive relief, actual damages, statutory damages, and any other relief the Court deems proper pursuant to the CCPA, such as costs and attorneys' fees.

COUNT X
CALIFORNIA CUSTOMER RECORDS ACT,
CAL. CIV. CODE § 1798.80, *et seq.*
(On Behalf of California Plaintiff and the California Subclass Against All Defendants)

140. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

141. Plaintiff Gianne (the "California Plaintiff") brings this Claim on behalf of herself and members of the California Subclass.

142. The California Customer Records Act ("CRA") was enacted "to ensure that personal information about California residents is protected." Cal. Civ. Code §1798.81.5(a)(1). The CRA requires that any business "that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code §1798.81.5(b).

143. Defendants own, maintain, and license personal information about California Plaintiff and the California subclass, as defined by the CRA.

144. Defendants failed to implement and maintain reasonable security procedures and practices to protect California Plaintiff's personal information from unauthorized access, destruction, use, modification, or disclosure, thereby violating the CRA.

145. As a direct and proximate result of Defendants' violation of the CRA, California Plaintiff's personal information was accessed without authorization in the Data Breach.

146. Further, Defendants did not timely notify California Plaintiff of the Data Breach, thereby violating the notice provisions of the CRA, which require that

"disclosure shall be made in the most expedient time possible and without unreasonable delay." Cal. Civ. Code §1798.82(a).

147. As a direct and proximate result of Defendants' violations of the CRA, California Plaintiff suffered damages and injury and is at high risk of suffering further damage and injury, including time and expenses related to monitoring her financial accounts and credit for fraudulent activity and increased risk of identity theft and fraud.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and

unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel

to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and controls, so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information,

as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their

confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

G. For such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: September 24, 2024

Respectfully submitted,

/s/ John Heenan

John Heenan
john@lawmontana.com
HEENAN & COOK
1631 Zimmerman Trail
Billings, Montana 59102
Tel: (406) 839-9091

Lesley E. Weaver*
Anne K. Davis*
Joshua D. Samra*
BLEICHMAR FONTI & AULD LLP
1330 Broadway, Suite 630
Oakland, California 94612
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com
adavis@bfalaw.com
jsamra@bfalaw.com

Gregory S. Mullens*
BLEICHMAR FONTI & AULD LLP
75 Virginia Road, 2nd Floor
White Plains, New York 10603
Tel.: (415) 445-4006
gmullens@bfalaw.com

Counsel for Plaintiff Natalie Gianne and the Proposed Class

** Pro Hac Vice application forthcoming*

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

Natalie Gianne

(b) County of Residence of First Listed Plaintiff Los Angeles, CA
(EXCEPT IN U.S. PLAINTIFF CASES)

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

John Heenan, Heenan & Cook, 1631 Zimmerman Trail
Billings, MT 59102, Tel: (406) 839-9091

DEFENDANTS

The Neiman Marcus Group LLC and Snowflake, Inc.

County of Residence of First Listed Defendant
(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
- [x] 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	[x] 4
Citizen of Another State	[x] 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
- [x] 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

INTELLECTUAL 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)*

- [x] 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)***:
Class Action Fairness Act, 28 U.S.C. § 1332

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: [x] Yes [ ] No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Brian Morris DOCKET NUMBER *See* Attachment A.

DATE Sept 24, 2024

SIGNATURE OF ATTORNEY OF RECORD /s/ John Heenan

FOR OFFICE USE ONLY

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

ATTACHMENT A
Related Cases

Cases	Judge
Leal v Snowflake, Inc., et al., 2:24-cv-00046-BMM	Hon. Brian Morris
Chaidez v. Snowflake, Inc., 2:24-cv-00050-BMM	Hon. Brian Morris
Doe, et al. v. Snowflake, Inc., 2:24-cv-00051-BMM	Hon. Brian Morris
Bowers v. Snowflake, Inc., 2:24-cv-00055-BMM	Hon. Brian Morris
Olivieri et al v. Snowflake, Inc., 2:24-cv-00056-BMM	Hon. Brian Morris
Wilkinson v. Snowflake, Inc., 2:24-cv-00057-BMM	Hon. Brian Morris
Armstrong v. Snowflake, 2:24-cv-00058-BMM	Hon. Brian Morris
Giangiulio v. Snowflake, 2:24-cv-00060-BMM	Hon. Brian Morris
Layman et al v. Snowflake, Inc., 2:24-cv-00062-BMM	Hon. Brian Morris
Lewis v. Snowflake et al, 2:24-cv-00064-BMM	Hon. Brian Morris
Mirvis v. Snowflake et al, 2:24-cv-00065-BMM	Hon. Brian Morris
Bryant-Booker v. Snowflake, 2:24-cv-00066-BMM	Hon. Brian Morris
Miller v. Snowflake, Inc. et al, 2:24-cv-00067-BMM	Hon. Brian Morris
Hornthal v. Snowflake, Inc. et al, 2:24-cv-00068-BMM	Hon. Brian Morris
Bobbitt v. Snowflake Inc. et al, 2:24-cv-00071-BMM	Hon. Brian Morris
Schwartz v. Snowflake, Inc., 2:24-cv-00074-BMM	Hon. Brian Morris
Rason v. Snowflake, Inc. et al, 2:24-cv-00076-BMM	Hon. Brian Morris
Townsend v. Snowflake, Inc. et al, 2:24-cv-00077-BMM	Hon. Brian Morris
Nader v. Snowflake, Inc. et al, 2:24-cv-00079-BMM	Hon. Brian Morris
Riley v. Snowflake, Inc., 2:24-cv-00084-BMM	Hon. Brian Morris
Wenze v. Snowflake, Inc., 2:24-cv-00088-BMM	Hon. Brian Morris
Fordham et al. v. Snowflake, Inc., 2:24-cv-00092-BMM	Hon. Brian Morris
Hollis v. Snowflake, Inc., 2:24-cv-00099-BMM	Hon. Brian Morris