HUNTON ANDREWS KURTH LLP
Ann Marie Mortimer (State Bar No. 169077)
amortimer@HuntonAK.com
Jason J. Kim (State Bar No. 221476)
kimj@HuntonAK.com
Brandon M. Marvisi (State Bar No. 329798)
bmarvisi@HuntonAK.com
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627
Telephone: (213) 532-2000
Facsimile: (213) 532-2020

Attorneys for Defendant
THE NEIMAN MARCUS GROUP LLC

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

CHRISTINA ZAIMI, individually. and on behalf of all others similarly situated,

Plaintiffs,

v.

THE NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company; and DOES 1-50, inclusive,

Defendants.

CASE NO.: 2:22-cv-02972

NOTICE OF REMOVAL OF ACTION PURSUANT TO 28 U.S.C. SECTIONS 1446, 1453 AND 1711

TO THE CLERK OF THE UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA:

PLEASE TAKE NOTICE that Defendant The Neiman Marcus Group LLC ("Neiman Marcus") hereby removes the state court action described below to this Court pursuant to 28 U.S.C. §§ 1446, 1453 and the Class Action Fairness Act of 2005, 28 U.S.C. § 1711, *et seq.* ("CAFA"). In support thereof, Neiman Marcus states as follows:

I.
INTRODUCTION

1. On January 12, 2022, Plaintiff Christina Zaimi filed this lawsuit in the Superior Court for the State of California, County of Los Angeles, styled as *Christina Zaimi v. The Neiman Marcus Group, LLC*, Case No. 22STCV01421 (the "State Action"). On April 22, 2022, Plaintiff filed the First Amended Complaint ("FAC"). The FAC in the State Action asserts three claims for: (1) violations of the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA"); (2) California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("Section 17200"); and (3) breach of contract. Each of Plaintiff's claims arises out of a data security incident that Neiman Marcus announced in September 2021 (the "Security Incident").

2. The Court in the State Action set an April 29, 2022 initial status conference. On April 19, 2022, the parties stipulated to continue that status conference until October 28, 2022 based on Neiman Marcus' intent to remove the State Action to this Court.

3. On April 20 2022, Plaintiff's counsel sent Neiman Marcus' counsel a Notice and Acknowledgment of Receipt, which Neiman Marcus' counsel executed and returned to Plaintiff's counsel that same day.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California90071-2627

4. On behalf of herself and the putative class, Plaintiff seeks, among other things, actual and punitive damages, statutory damages, restitution, and attorneys' fees. FAC, Prayer.

5. As shown below, the State Action is removable to this Court because all procedural requirements for removal are satisfied, and this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d).

II.

NEIMAN MARCUS HAS SATISFIED THE PROCEDURAL REQUIREMENTS FOR REMOVAL

6. Pursuant to 28 U.S.C. § 1446(b), the "notice of removal of a civil action or proceeding shall be filed within thirty days after the receipt by the defendant, through service or otherwise, of a copy of the initial pleading setting forth the claim for relief upon which such action or proceeding is based." As stated above, Neiman Marcus returned to Plaintiffs' counsel an executed Notice and Acknowledgment of Receipt on April 20 2022. Cal. Civ. Proc. Code § 415.30(c). Thus, Neiman Marcus' Notice of Removal is timely because it is filed within 30 days of that date. *Murphy Bros. v. Michetti Pipe Stringing, Inc.*, 526 U.S. 344 (1999).

7. Venue lies in the United States District Court for the Central District of California because Plaintiff filed the State Action in this District. *See* 28 U.S.C. § 1441(a) (mandating venue for removal actions).

8. Pursuant to 28 U.S.C. § 1446(a), a copy of all process, pleadings, and orders served on Neiman Marcus, which papers include the Summons and Class Action Complaint, are concurrently filed as attachments hereto.

9. Pursuant to 28 U.S.C. § 1446(d), a copy of this Notice of Removal is being served on counsel for Plaintiff, and a copy is being filed with the Clerk of the Superior Court for the State of California, County of Los Angeles.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California90071-2627

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California90071-2627

III.

REMOVAL IS PROPER BECAUSE THIS COURT HAS SUBJECT MATTER JURISDICTION UNDER CAFA

10. The State Action is a civil action over which this Court has original jurisdiction pursuant to CAFA. Under CAFA, federal courts have original jurisdiction over a class action if: (i) it involves 100 or more putative class members; (ii) any class member is a citizen of a State different from any defendant; and (iii) the aggregated amount in controversy exceeds $5,000,000, exclusive of interest and costs. *See* 28 U.S.C. § 1332(d). The State Action meets those requirements.

11. To remove a case under CAFA, a defendant need only "file in the federal forum a notice of removal 'containing a short and plain statement of the grounds for removal'"—*i.e.*, the same liberal pleading standard required by Federal Rule of Civil Procedure 8(a), requiring only plausible allegations as to the basis for removal. *Dart Cherokee Basin Operating Co., LLC v. Owens*, 135 S. Ct. 547, 553 (2014) (quoting 28 U.S.C. § 1446(a)). Neiman Marcus easily meets that standard.

12. As set forth below, this is a putative class action in which, as alleged: (i) there are more than 100 members in Plaintiff's proposed class; (ii) Plaintiff and the members of the putative class have a different citizenship than Neiman Marcus; and (iii) the claims of the proposed class members exceed the sum or value of $5,000,000 in the aggregate, exclusive of interest and costs. Accordingly, this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d).

A. The State Action Is a "Class Action" Under CAFA

13. CAFA defines a "class action" as "any civil action filed under rule 23 of the Federal Rules of Civil Procedure or similar State statute or rule or judicial procedure authorizing an action to be brought by 1 or more representative persons as a class action." 28 U.S.C. § 1332(d)(1)(B).

14. Here, Plaintiff styles her Complaint as a "Class Action Complaint;" she specifically alleges that she is bringing the State Action "on behalf of herself and all

affected California residents" (FAC ¶ 6); she purports to set forth class action allegations under Section 382 of the California Code of Civil Procedure and Cal. Civ. Code § 1781 (*id.* ¶¶ 45-53); she contends a "class action is superior to any other available method for the fair and efficient adjudication of this controversy" (*id.* ¶ 52); and she seeks an order certifying this action as a class action, designating Plaintiff as the representative of the Class, and appointing Plaintiff's counsel as counsel for the Class (*id.*, Prayer). Actions seeking class treatment in this manner are "class actions" under CAFA. *Bryant v. NCR Corp.*, 284 F. Supp. 3d 1147, 1150 (S.D. Cal. 2018) ("Here, there is no dispute the present action is a 'class action' under CAFA, as the action contains class allegations under California Code of Civil Procedure § 382.").

B. The Putative Class Consists of More than 100 Members

15. Plaintiff seeks to represent a class defined as: "All California residents whose PII or PCD was subjected to the Data Breach." FAC ¶ 45.

16. The putative class consists of more than 100 individuals. Indeed, Plaintiff alleges that "[w]hile the exact number of class members is unknown," "reports estimate the breach to include 4.6 million compromised accounts containing PII of Neiman Marcus customers, including Plaintiff and Class Members." FAC ¶ 48. Moreover, Plaintiff bases her claims on a notice Neiman Marcus sent to customers potentially impacted by the Security Incident. *Id.* ¶ 36. Neiman Marcus avers that it sent such notices to more than 50,000 individuals with California addresses. Accordingly, the requirement of 100 or more class members is met.

C. Minimal Diversity Exists

17. Under CAFA's "minimal diversity" requirement, a "federal court may exercise jurisdiction over a class action if 'any member of a class of plaintiffs is a citizen of a State different from any defendant.'" *Mississippi ex rel. Hood v. AU Optronics Corp.*, 134 S. Ct. 736, 740 (2014) (quoting 28 U.S.C. § 1332(d)(2)(A)); *Duran v. Fernandez Bros., Inc.*, 2015 WL 7012884, at *3 (N.D. Cal. Nov. 12, 2015).

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California90071-2627

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California90071-2627

18. Under CAFA, minimal diversity exists if any member of the proposed class is a citizen of a State other than Texas. 28 U.S.C. § 1332(d)(2)(A), (d)(2)(B); *Mississippi ex rel. Hood*, 134 S. Ct. at 740; *Duran*, 2015 WL 7012884, at *3. CAFA's minimal diversity requirement is readily satisfied here.

19. Neiman Marcus avers that it is a Delaware limited liability company that has its principal place of business in Dallas, Texas. Neiman Marcus, therefore, is a citizen of both Delaware and Texas for removal purposes. *Hertz Corp. v. Friend*, 559 U.S.77, 80-81 (2010); 28 U.S.C. § 1332(c)(1); *see also Pae v. Fox Rest. Concepts, LLC*, 2017 WL 3184464, at *2 (C.D. Cal. July 25, 2017) (under CAFA, a limited liability corporation "'shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized.'") (quoting 28 U.S.C. § 1332(d)(10)).[1]

20. Neiman Marcus further avers that Plaintiff is a California citizen, thereby making her diverse from Neiman Marcus. Indeed Plaintiff claims she has "resided in Los Angeles County, California" "[a]t all relevant times." FAC ¶ 11. Moreover, Plaintiff purports to represent a California Class consisting of "all affected California residents." *Id.* ¶ 6. Accordingly, at least one member of the proposed class is a citizen of a State other than Texas or Delaware. Minimal diversity exists.

D. <u>The Amount-in-Controversy Requirement Is Satisfied</u>

21. To establish CAFA's amount-in-controversy requirement, Neiman Marcus "need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold" of $5 million. *Dart Cherokee*, 135 S. Ct. at 554.

22. Although Neiman Marcus denies Plaintiff or any putative class member suffered any cognizable injury as a result of the incident at issue, Plaintiff asserts causes of action for violations of the CCPA and Section 17200, as well as breach of contract. FAC ¶¶ 54-78.

---

[1] In any event, Neiman Marcus' lone member, NMG Holding Company, Inc., is a Delaware corporation with its principal place of business in Texas.

23. In connection with the CCPA claim alone, Plaintiff is "pursu[ing] the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater." FAC ¶ 64.

24. Given the putative class consists of more than 50,000 individuals, and even assuming the low-end $100 per violation statutory recovery, CAFA's $5 million amount-in-controversy requirement is met on Plaintiff's CCPA claim alone.

WHEREFORE, Neiman Marcus respectfully removes the State Action to this Court pursuant to 28 U.S.C. § 1441(b).

Dated: May 4, 2022

HUNTON ANDREWS KURTH LLP

By: /s/ Ann Marie Mortimer
Ann Marie Mortimer
Jason J. Kim
Brandon Marvisi
Attorneys for Defendant
THE NEIMAN MARCUS GROUP LLC

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California90071-2627

KAZEROUNI LAW GROUP, APC
ABBAS KAZEROUNIAN (SBN 249203)
MONA AMINI (SBN 296829)
245 Fischer Avenue, Unit D1
Costa Mesa, CA 92626
Tel: (800) 400-6808
Fax: (800) 520-5523
ak@kazlg.com
mona@kazlg.com

[Additional Plaintiff's Counsel on Signature Page]

Attorneys for Plaintiff,
Christina Zaimi and the putative class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES – COMPLEX CIVIL

CHRISTINA ZAIMI, individually. and on behalf of all others similarly situated,

Plaintiffs,

v.

THE NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company; and DOES 1-50, inclusive,

Defendants.

Case No. 22STCV01421

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*; and
3. BREACH OF CONTRACT

DEMAND FOR JURY TRIAL

///

///

///

///

///

///

///

///

///

Plaintiff CHRISTINA ZAIMI ("Plaintiff"), individually and on behalf of the general public and all others similarly situated ("Class members"), by and through her attorneys, upon personal knowledge as to facts pertaining to herself and on information and belief as to all other matters, brings this class action against Defendant, THE NEIMAN MARCUS GROUP, LLC ("Defendant" or "Neiman Marcus"), and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action against The Neiman Marcus Group, LLC and its related entities, subsidiaries and agents for failing to secure and safeguard the personally identifiable information ("PII") and payment card data ("PCD") that Defendant collected and maintained (collectively "Private Information"), and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been stolen (the "Data Breach"). Neiman Marcus, which includes Neiman Marcus, Neiman Marcus Direct, Horchow, Last Call, and Bergdorf Goodman, is a nationwide retailer ranked 502nd on the Fortune 1,000 list. For its business purposes, Neiman Marcus stores a substantial amount of personally identifiable information ("PII") from customers.

2. On or about September 30, 2021, Neiman Marcus announced that an unauthorized party had gained access to its data systems and stole customer information including customer names and contact information, payment credit card numbers and expiration date, Neiman Marcus virtual gift card number, and the username, password, and security questions and answers associated with Neiman Marcus online accounts (the "Data Breach")[1]. The Neiman Marcus database accessed in the Data Breach reportedly contained approximately 4.6 million individual customer records containing PII and payment card data .

3. Although the Data Breach occurred in May 2020 placing sensitive customer information in the hands of malicious actors, Neiman Marcus waited over 16 months until September 30, 2021 to notify customers. This notice was still lacking in information necessary for Plaintiff and Class members to understand the scope and severity of the Data Breach.

[1] *See* https://www.neimanmarcus.com/editorial/security/online-accounts

4. Defendant owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected from its customers for business purposes and stored on its networks.

5. Defendant breached that duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII and PCD from unauthorized access and storing and retaining Plaintiff's and Class members' personal information on inadequately protected networks.

6. The Data Breach happened because of Defendant's inadequate cybersecurity, which caused Plaintiff's and Class members' PII and PCD to be accessed, exfiltrated and disclosed. This action seeks to remedy these failings. Plaintiff brings this action on behalf of herself and all affected California residents.

7. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for herself and the Class, injunctive relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

8. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and Class members pursuant to Cal. Code Civ. Proc. § 382.

9. This Court has personal jurisdiction over Defendant because Defendant's has retail stores in California and regularly conducts business is in California.

10. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Defendant regularly conducts business in this county, and unlawful acts or omissions have occurred in this county.

PARTIES

11. At all relevant times, Plaintiff resided in Los Angeles County, California. Plaintiff is a consumer who has shopped numerous times from Neiman Marcus stores and has used her credit card(s) to make purchases at a Neiman Marcus store in this county, through Neiman Marcus' website, and/or her Neiman Marcus online account. Plaintiff has made several purchases from Neiman Marcus both prior to and after the May 2020 data breach.

12. Plaintiff provided her PII and PCD to Neiman Marcus as part of Neiman Marcus's in store sales and online sales services, including her name, telephone number, date of birth, email address, physical address, and gender. Plaintiff also created an account password and provided personal answers to the security questions.

13. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiff's PII and/or PCD was accessed and exfiltrated, stolen and otherwise disclosed to unauthorized persons in the Data Breach.

14. The Neiman Marcus Group, LLC is a limited liability company organized under the laws of the state of Delaware, with its principal place of business located at One Marcus Square, 1618 Main Street, Dallas Texas, 75201.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

15. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[2] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

16. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[3]

---

[2] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[3] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

17. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[4] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

18. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[5]

19. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

20. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[6] This business has created a new market for the sale and purchase of this valuable data.[7]

---

[4] *See* Soma, *Corporate Privacy Trend, supra*.

[5] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

[6] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[7] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

21. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

22. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[9]

23. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

24. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

25. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[10]

26. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's

---

[8] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1# page_scan_tab_contents.

[9] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[10] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

name.[11] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

27. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[12]

28. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[14]

29. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[15] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[16] And in 2019, Javelin Strategy &

---

[11] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[12] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[14] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[15] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[16] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[17]

30. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[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."

31. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[18]

32. It is within this context that Plaintiff and thousands of Neiman Marcus customers must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Neiman Marcus's Collection of Customers' PII

33. Neiman Marcus acknowledges that it stores and transmits a substantial amount of confidential, personal, and other sensitive information from its customers. The type of information is detailed in Neiman Marcus's Privacy Policy (last updated June 30, 2020),[19] which for California customers, identifies the categories of personal information it may have collected about them over the past 12 months and which information is covered by the California Consumer Privacy Act ("CCPA") as follows:

---

[17] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[18] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[19] *See* Neiman Marcus's Privacy Policy, *available at* https://www.neimanmarcus.com/c/Assistance/Privacy-Policy-Terms-of-Use-cat33940739.

- Personal Identifiers – such as name, postal address, Internet Protocol address, email address, social security number, driver's license number, passport number, or other similar identifiers.

- Protected Characteristics, such as gender.

- Commercial information – such as records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

- Internet or other electronic network activity information, including browsing and search history

- Geolocation data

- Audio, electronic, visual, information

- Inferences drawn from any of the information identified below, to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

34. Neiman Marcus's Privacy Policy – Security and Privacy says that it may collect names, addresses, telephone number, birth date, email address, credit card account numbers, driver's license numbers, information such as one's interests or product preferences, purchase information such as specific products or services purchased or used and preferences, interests, sizing and favorite brands.

Neiman Marcus Promises to Safeguard Customer PII

35. Neiman Marcus's Privacy Policy promises customers 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."

The Data Breach

36. On September 30, 2021, Neiman Marcus sent official notice of the Data Breach to customers stating "Earlier this month, we learned that in May 2020 an unauthorized party obtained personal information associated with certain of our customers' online accounts."

37. According to Neiman Marcus, "The personal information for affected customers varied and may have included your name and contact information; payment card number and expiration date(without CVV number); Neiman Marcus virtual gift card number (without PIN); and the username, password, and security questions and answers associated with your Neiman Marcus online account."

38. Neiman Marcus also claimed to have immediately launched its own investigation, hired a cybersecurity consultant, and contacted law enforcement.

39. News reports about the Data Breach provide more details than offered by Neiman Marcus. For instance, Neiman Marcus provided no information about how many subscribers were affected by the Data Breach whereas new media reports estimate 4.6 million compromised customers.

Defendants Knew or Should Have Known PII Are High Risk Targets

40. Defendants knew or should have known that PII like that at issue here, are high risk targets for identity thieves.

41. The Identity Theft Resource Center reported that the banking/credit/financial sector had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135 data breaches exposing at least 1,709,013 million records in 2018.[20]

42. Prior to the breach there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a

[20] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in May 2019, First American Financial reported a security incident on its website that potentially exposed 885 million real estate and mortgage related documents, among others. Across industries, financial services has the second-highest cost per breached record, behind healthcare. In financial services, an average breach costs $210 per record, while a "mega breach," like Capital One's, can cost up to $388 per record.[21]

43. Anurag Kahol, CTO of Bitglass recently commented that "[g]iven that organizations in the financial services industry are entrusted with highly valuable, personally identifiable information (PII), they represent an attractive target for cybercriminals[.]" HelpNetSecurity reports that "[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."[22]

44. Neiman Marcus has previously been sued in 2014 for a similar albeit smaller data breach when it allowed hackers to steal payment information collected between July 16, 2013 and Oct. 30, 2013 from approximately 350,000 customers.

45. As such, Defendant was aware that PII and PCD is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' PII against cyber-security attacks that Defendant should have anticipated and guarded against.

---

[21] Samantha Ann Schwartz, *62% of breached data came from financial services in 2019*, CioDive (Dec. 23, 2019), *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/.

[22] HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), *available at* https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/.

CLASS DEFINITION AND ALLEGATIONS

46. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks certification of a class defined as: ***All California residents whose PII or PCD was subjected to the Data Breach.***

47. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

48. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

49. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, Defendant acknowledges the Data Breach, and reports estimate the breach to include 4.6 million compromised accounts containing PII of Neiman Marcus customers, including Plaintiff and Class members. Plaintiff therefore believes that the Class is so numerous that joinder of all members is impractical.

50. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII and/or PCD compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

51. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected from Plaintiff and Class members;

(b) Whether Defendant breached its duty to protect the PII of Plaintiff and each Class member; and

(c) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

52. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to or that conflicts with the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

53. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

54. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

55. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

56. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[23]

57. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

58. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party 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." 1798.81.5(c).

---

[23] CALIFORNIA CONSUMER PRIVACY ACT (CCPA) COMPLIANCE, https://buyergenomics.com/ccpa-complience/.

59. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

60. Plaintiff and Class members' are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

61. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in and is headquartered in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

62. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and Class members' unencrypted first and last names and encrypted Social security numbers, among other information.

63. Plaintiff's PII and/or PCD was subject to unauthorized access and exfiltration, theft or disclosure because her PII, including name and contact information, and payment card information was wrongfully accessed and taken by unauthorized persons.

64. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of Plaintiff's and Class members' PII as a result of this attack.

65. On January 12, 2022, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Ex. A. If Defendant does not cure the violation within 30 days, Plaintiff will amend her complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

66. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual damages, injunctive relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

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

68. 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, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

69. In the course of conducting its business, Defendant 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, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

70. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

71. Defendant's 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 Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's 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 CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

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

73. As a direct and proximate result of Defendant's 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 under the CCPA, (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.

74. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its 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.

THIRD CAUSE OF ACTION

Breach of Contract

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

76. Plaintiff and Class members entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

77. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their purchases of Neiman Marcus's products and services.

78. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

79. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

80. **Damages.** As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members suffered (and will continue to suffer) actual damages and other injury and harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and 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) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages. Plaintiff and Class members also are entitled to equitable relief, including, without limitation, restitution. Plaintiff's and Class members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

81. **Punitive Damages**. Plaintiff and Class members also are entitled to punitive damages from Defendant, as punishment and to deter such wrongful conduct. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

82. **Injunctive Relief**. Pursuant to, *inter alia*, the CCPA and the UCL, Plaintiff and Class members also are entitled to injunctive relief in multiple forms including, without limitation, (i) credit monitoring, (ii) Internet monitoring, (iii) identity theft insurance, (iv) prohibiting Defendant from continuing its above-described wrongful conduct, (v) requiring Defendant to modify its corporate culture and implement and maintain reasonable security procedures and practices to safeguard and protect the PII entrusted to it, (vi) periodic compliance audits by a third party to ensure that Defendant is properly safeguarding and protecting the PII in its possession,

custody and control, and (vii) clear and effective notice to Class members about the serious risks posed by the exposure of their personal information and the precise steps that must be taken to protect themselves. All conditions precedent to Plaintiff's and Class members' claims for relief have been performed and occurred.

83. **Attorneys' Fees, Litigation Expenses and Costs**. Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action.

WHEREFORE, Plaintiff, on behalf of herself and all members of the Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the Class. Plaintiff, on behalf of herself and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit; and

(vii) such other and further relief the Court deems just and proper.

///

///

///

///

///

///

///

///

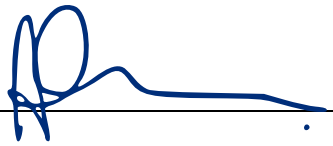
DEMAND FOR JURY TRIAL

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

Respectfully submitted,

Dated: January 12, 2022

KAZEROUNI LAW GROUP, APC

By: 

Abbas Kazerounian (SBN 249203)
Mona Amini (SBN 296829)
245 Fischer Avenue, Unit D1
Costa Mesa, CA 92626
Tel.: (800) 400-6808
Fax: (800) 520-5523
ak@kazlg.com
mona@kazlg.com

/s/ William F. Cash III
William F. Cash III (*pro hac vice motion forthcoming*)
Scott Warrick (*pro hac vice motion forthcoming*)
LEVIN, PAPANTONIO, RAFFERTY, PROCTOR, BUCHANAN, O'BRIEN, BARR & MOUGEY, P.A.
316 South Baylen Street, Suite 600
Pensacola, FL 32502
Phone: 850-435-7059
Fax: 850-435-7020
Email: bcash@levinlaw.com
Email: swarrick@levinlaw.com

Attorneys for Plaintiff and the putative class

EXHIBIT A

KAZEROUNI LAW GROUP, APC

245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

January 12, 2022

VIA CERTIFIED MAIL
The Neiman Marcus Group, LLC
Attn: Legal Department
1618 Main Street
Dallas, TX 75201

Re: Christina Zaimi, et al. v. The Neiman Marcus Group, LLC, et al.

To Whom It May Concern:

We represent Plaintiff Christina Ziaimi ("Plaintiff") and all other similarly situated consumers in a putative class action against The Neiman Marcus Group, LLC ("Neiman Marcus") arising out of, *inter alia*, Neiman Marcus' failure to provide reasonable security for Plaintiff's and the proposed class members' personal information and payment card information, which resulted in the unauthorized access, theft, or disclosure of this information (the "Data Breach"). To our knowledge the Data Breach occurred sometime during May 2020.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff's Class Action Complaint, a copy of which is attached and incorporated by reference. Neiman Marcus' conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Class Action Complaint constitute sufficient notice of the claims asserted against Neiman Marcus, pursuant to California Civil Code 1798.150(b)(1), Plaintiff demands that, in the event a cure is possible, Neiman Marcus is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within 30 days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]

KAZEROUNI LAW GROUP, APC
ABBAS KAZEROUNIAN (SBN 249203)
MONA AMINI (SBN 296829)
245 Fischer Avenue, Unit D1
Costa Mesa, CA 92626
Tel: (800) 400-6808
Fax: (800) 520-5523
ak@kazlg.com
mona@kazlg.com

[Additional Plaintiff's Counsel on Signature Page]

Attorneys for Plaintiff,
Christina Zaimi and the putative Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES – COMPLEX CIVIL

CHRISTINA ZAIMI, individually. and on behalf of all others similarly situated,

Plaintiff,

v.

THE NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company; and DOES 1-50, inclusive,

Defendants.

Case No.: 22STCV01421
Assigned for All Purposes to:
Judge Hon. Carolyn B. Kuhl
Dept. 12

CLASS ACTION

AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*; and
3. BREACH OF CONTRACT

Action Filed: January 12, 2022
Trial Date: TBD

DEMAND FOR JURY TRIAL

//

//

//

//

//

//

Plaintiff CHRISTINA ZAIMI ("Plaintiff"), individually and on behalf of the general public and all others similarly situated ("Class members"), by and through her attorneys, upon personal knowledge as to facts pertaining to herself and on information and belief as to all other matters, brings this class action against Defendant, THE NEIMAN MARCUS GROUP, LLC ("Defendant" or "Neiman Marcus"), and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action against The Neiman Marcus Group, LLC and its related entities, subsidiaries and agents for failing to secure and safeguard the personally identifiable information ("PII") and payment card data ("PCD") that Defendant collected and maintained (collectively "Private Information"), and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been stolen (the "Data Breach"). Neiman Marcus, which includes Neiman Marcus, Neiman Marcus Direct, Horchow, Last Call, and Bergdorf Goodman, is a nationwide retailer ranked 502nd on the Fortune 1,000 list. For its business purposes, Neiman Marcus stores a substantial amount of personally identifiable information ("PII") from customers.

2. On or about September 30, 2021, Neiman Marcus announced that an unauthorized party had gained access to its data systems and stole customer information including customer names and contact information, payment credit card numbers and expiration date, Neiman Marcus virtual gift card number, and the username, password, and security questions and answers associated with Neiman Marcus online accounts (the "Data Breach")[1]. The Neiman Marcus database accessed in the Data Breach reportedly contained approximately 4.6 million individual customer records containing PII and payment card data.

3. Although the Data Breach occurred in May 2020 placing sensitive customer information in the hands of malicious actors, Neiman Marcus waited over 16 months until September 30, 2021, to notify customers. This notice was still lacking in information necessary for Plaintiff and Class members to understand the scope and severity of the Data Breach.

[1] *See* https://www.neimanmarcus.com/editorial/security/online-accounts

4. Defendant owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected from its customers for business purposes and stored on its networks.

5. Defendant breached that duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII and PCD from unauthorized access and storing and retaining Plaintiff's and Class members' personal information on inadequately protected networks.

6. The Data Breach happened because of Defendant's inadequate cybersecurity, which caused Plaintiff's and Class members' PII and PCD to be accessed, exfiltrated and disclosed. This action seeks to remedy these failings. Plaintiff brings this action on behalf of herself and all affected California residents.

7. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for herself and the Class, statutory damages, injunctive relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

8. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and Class members pursuant to Cal. Code Civ. Proc. § 382.

9. This Court has personal jurisdiction over Defendant because Defendant's has retail stores in California and regularly conducts business is in California.

10. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Defendant regularly conducts business in this county, and unlawful acts or omissions have occurred in this county.

PARTIES

11. At all relevant times, Plaintiff resided in Los Angeles County, California. Plaintiff is a consumer who has shopped numerous times from Neiman Marcus stores and has used her credit card(s) to make purchases at a Neiman Marcus store in this county, through Neiman Marcus'

website, and/or her Neiman Marcus online account. Plaintiff has made several purchases from Neiman Marcus both prior to and after the May 2020 data breach.

12. Plaintiff provided her PII and PCD to Neiman Marcus as part of Neiman Marcus's in store sales and online sales services, including her name, telephone number, date of birth, email address, physical address, and gender. Plaintiff also created an account password and provided personal answers to the security questions.

13. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiff's PII and/or PCD was accessed and exfiltrated, stolen and otherwise disclosed to unauthorized persons in the Data Breach.

14. The Neiman Marcus Group, LLC is a limited liability company organized under the laws of the state of Delaware, with its principal place of business located at One Marcus Square, 1618 Main Street, Dallas Texas, 75201.

ADDITIONAL FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

15. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[2] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

16. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[3]

---

[2] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[3] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

17. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[4] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

18. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[5]

19. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list."

20. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[6] This business has created a new market for the sale and purchase of this valuable data.[7]

21. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is

---

[4] *See* Soma, *Corporate Privacy Trend, supra*.
[5] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.
[6] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.
[7] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576 160764037920274.

considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

22. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[9]

23. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

24. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

25. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[10]

26. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[11] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

---

[8] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#.

[9] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[10] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[11] *See* GAO, GAO Report 9 (2007) *available at* http://www.gao.gov/new.items/d07737.pdf.

27. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[12]

28. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[14]

29. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[15] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft—a common result of data breaches—was $298 dollars.[16] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[17]

---

[12] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[14] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[15] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[16] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[17] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

30. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [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.

31. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[18]

32. It is within this context that Plaintiff and thousands of Neiman Marcus customers must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Neiman Marcus's Collection of Customers' PII

33. Neiman Marcus acknowledges that it stores and transmits a substantial amount of confidential, personal, and other sensitive information from its customers. The type of information is detailed in Neiman Marcus's Privacy Policy (last updated June 30, 2020),[19] which for California customers, identifies the categories of personal information it may have collected about them over the past 12 months and which information is covered by the California Consumer Privacy Act ("CCPA") as follows:

- Personal Identifiers – such as name, postal address, Internet Protocol address, email address, social security number, driver's license number, passport number, or other similar identifiers.
- Protected Characteristics, such as gender.
- Commercial information – such as records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

---

[18] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[19] *See* Neiman Marcus's Privacy Policy, *available at* https://www.neimanmarcus.com/c/Assistance/Privacy-Policy-Terms-of-Use-cat33940739.

- Internet or other electronic network activity information, including browsing and search history.
- Geolocation data.
- Audio, electronic, visual, information.
- Inferences drawn from any of the information identified below, to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

34. Neiman Marcus's Privacy Policy – Security and Privacy says that it may collect names, addresses, telephone number, birth date, email address, credit card account numbers, driver's license numbers, information such as one's interests or product preferences, purchase information such as specific products or services purchased or used and preferences, interests, sizing and favorite brands.

Neiman Marcus Promises to Safeguard Customer PII

35. Neiman Marcus's Privacy Policy promises customers 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."

The Data Breach

36. On September 30, 2021, Neiman Marcus sent official notice of the Data Breach to customers stating, "Earlier this month, we learned that in May 2020 an unauthorized party obtained personal information associated with certain of our customers' online accounts."

37. According to Neiman Marcus, "The personal information for affected customers varied and may have included your name and contact information; payment card number and expiration date (without CVV number); Neiman Marcus virtual gift card number (without PIN); and the username, password, and security questions and answers associated with your Neiman Marcus online account."

38. Neiman Marcus also claims to have immediately launched its own investigation, hired a cybersecurity consultant, and contacted law enforcement.

39. News reports about the Data Breach provide more details than offered by Neiman Marcus. For instance, Neiman Marcus provided no information about how many subscribers were affected by the Data Breach, whereas new media reports estimate 4.6 million compromised customers.

Defendants Knew or Should Have Known PII Are High Risk Targets

40. Defendants knew or should have known that PII like that at issue here, are high risk targets for identity thieves.

41. The Identity Theft Resource Center reported that the banking/credit/financial sector had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135 data breaches exposing at least 1,709,013 million records in 2018.[20] Further, the ITRC identified "hacking" as the most common form of data breach in 2018, accounting for 39% of data breaches.

42. Prior to the breach there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in May 2019, First American Financial reported a security incident on its website that potentially exposed 885 million real estate and mortgage related documents, among others. Across industries, financial services has the second-highest cost per breached record, behind healthcare. In financial services, an average breach costs $210 per record, while a "mega breach," like Capital One's, can cost up to $388 per record.[21]

---

[20] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[21] Samantha Ann Schwartz, *62% of breached data came from financial services in 2019*, CioDive (Dec. 23, 2019), *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/.

43. Anurag Kahol, CTO of Bitglass recently commented that "[g]iven that organizations in the financial services industry are entrusted with highly valuable, personally identifiable information (PII), they represent an attractive target for cybercriminals[.]" HelpNetSecurity reports that "[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."[22]

44. Defendant was aware that PII and PCD is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' PII against cyber-security attacks that Defendant should have anticipated and guarded against.

CLASS DEFINITION AND ALLEGATIONS

45. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks to represent and intends to move for certification of a class defined as:

All California residents whose PII or PCD was subjected to the Data Breach.

46. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

47. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

48. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of

[22] HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), *available at* https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/.

Class members is unknown, Defendant acknowledges the Data Breach, and reports estimate the breach to include 4.6 million compromised accounts containing PII of Neiman Marcus customers, including Plaintiff and Class members. Plaintiff therefore believes that the Class is so numerous that joinder of all members is impractical.

49. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII and/or PCD compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

50. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected from Plaintiff and Class members;

b) Whether Defendant breached its duty to protect the PII of Plaintiff and each Class member; and

c) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

51. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to or that conflicts with the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

52. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible

for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

53. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

54. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

55. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[23]

56. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are

[23] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

57. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party 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." 1798.81.5(c).

58. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

59. Plaintiff and Class members' are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

60. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) does business in and is headquartered in California; and

d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or

devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

61. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and Class members' unencrypted first and last names, contact information, payment card number and expiration date, and the username, password, and security questions and answers associated with their Neiman Marcus online account,, among other information.

62. Plaintiff's PII and/or PCD was subject to unauthorized access and exfiltration, theft or disclosure because her PII, including name and contact information, and payment card information was wrongfully accessed and taken by unauthorized persons.

63. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of Plaintiff's and Class members' PII as a result of this attack.

64. On January 12, 2022, Plaintiff provided written notice to Defendant identifying the specific provisions of the CCPA Plaintiff alleges Defendant has violated. Defendant has not cured the violation within thirty (30) days thereof. Accordingly, Plaintiff amends the complaint to additionally pursue the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

65. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual and statutory damages, injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*

66. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

67. 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, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

68. In the course of conducting its business, Defendant 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, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

69. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

70. Defendant's 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 Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and

unscrupulous. Defendant's 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 CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

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

72. As a direct and proximate result of Defendant's 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 under the CCPA, (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.

73. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its 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.

THIRD CAUSE OF ACTION

Breach of Contract

74. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

75. Plaintiff and Class members entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

76. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their purchases of Neiman Marcus's products and services.

77. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

78. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

79. **Damages.** As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members are entitled to statutory damages pursuant to Cal. Civ. Code § 1798.150(a)(1)(A) and have suffered (and will continue to suffer) actual damages and other injury and harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and 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) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages. Plaintiff and Class members also are entitled to equitable relief, including, without limitation, restitution. Plaintiff's and Class members'

damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

80. **Punitive Damages**. Plaintiff and Class members also are entitled to punitive damages from Defendant, as punishment and to deter such wrongful conduct. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

81. **Injunctive Relief**. Pursuant to, *inter alia*, the CCPA and the UCL, Plaintiff and Class members also are entitled to injunctive relief in multiple forms including, without limitation, (i) credit monitoring, (ii) Internet monitoring, (iii) identity theft insurance, (iv) prohibiting Defendant from continuing its above-described wrongful conduct, (v) requiring Defendant to modify its corporate culture and implement and maintain reasonable security procedures and practices to safeguard and protect the PII entrusted to it, (vi) periodic compliance audits by a third party to ensure that Defendant is properly safeguarding and protecting the PII in its possession, custody and control, and (vii) clear and effective notice to Class members about the serious risks posed by the exposure of their personal information and the precise steps that must be taken to protect themselves. All conditions precedent to Plaintiff's and Class members' claims for relief have been performed and occurred.

82. **Attorneys' Fees, Litigation Expenses and Costs**. Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action.

WHEREFORE, Plaintiff, on behalf of herself and all members of the Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the Class. Plaintiff, on behalf of herself and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) statutory damages;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit; and

(vii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and all members of the Class, hereby demands a jury trial on all issues so triable.

Dated: April 11, 2022

KAZEROUNI LAW GROUP, APC

By: _____

Abbas Kazerounian, Esq.
Mona Amini, Esq.
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
ak@kazlg.com
mona@kazlg.com

/s/ William F. Cash III
William F. Cash III (*pro hac vice motion forthcoming*)
Scott Warrick (*pro hac vice motion forthcoming*)
LEVIN, PAPANTONIO, RAFFERTY, PROCTOR, BUCHANAN, O'BRIEN, BARR & MOUGEY, P.A.
316 South Baylen Street, Suite 600
Pensacola, FL 32502
Phone: 850-435-7059
Fax: 850-435-7020
Email: bcash@levinlaw.com
Email: swarrick@levinlaw.com

ClassAction.org
