UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

HILARY REMIJAS and JOANNE KAO, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

THE NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company,

Defendant.

Case No. 1:14-cv-1735

Hon. Sharon Johnson Coleman

SECOND AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs HILARY REMIJAS ("Remijas") and JOANNE KAO ("Kao") (collectively, "Plaintiffs") bring this action against Defendant THE NEIMAN MARCUS GROUP, LLC ("Neiman Marcus" or "Defendant"), a Delaware limited liability company, on behalf of themselves and all others similarly situated to obtain damages, restitution and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant 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 and precisely what types of information were stolen (the "Data Breach").

2. Due to Defendant's negligence, the Private Information that Defendant collected and maintained is now in the hands of thieves. Accordingly, Plaintiffs bring this action against Defendant asserting claims for negligence, violation of N.Y. G.B.L. § 349 and 815 ILCS 505/1, Breach of Implied Contract, Violation of California Unfair Competition Law, Business & Professions Code § 17200, Invasion of Privacy, Bailment and Conversion under California law, violation of California Civil Code § 1798.80 *et. seq*., and violation of the Fair Credit Reporting Act, codified at 15 U.S.C. § 1681 *et. seq*.

PARTIES

3. Plaintiff Remijas is a current resident of Illinois. Ms. Remijas made purchases using a Neiman Marcus credit card at a Neiman Marcus location in Oak Brook, Illinois on August 7, 2013 and December 21, 2013. Ms. Remijas did not receive any notice from Defendant about the Data Breach.

4. Plaintiff Kao is a current resident of California. Ms. Kao made purchases at a Neiman Marcus retail location in San Francisco, California on: February 25, March 15, April 13, April 19, May 2, June 19, October 1, October 11, November 11, and December 31, 2013. On January 7, 2014, Ms. Kao received an email from Chase Bank that her debit card had been compromised and that a new card would be issued to replace the compromised card. In January 2014, she received a notice letter from Defendant about the Data Breach.

5. Defendant The Neiman Marcus Group, LLC ("Defendant") is a Delaware limited liability company headquartered in Dallas, Texas. Defendant operates retail stores within this District, including on North Michigan Avenue. Defendant allowed a massive breach of personal and financial information it collected and maintained to occur in 2013, which is the subject of this Complaint.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), the class contains members of diverse citizenship from Defendant, and the amount in controversy exceeds $5 million.

7. This Court has personal jurisdiction over Defendant because Defendant is authorized to and does conduct substantial business in Illinois, and in this District.

Defendant owns and operates two retail locations within this District and in another location in the state of Illinois.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to this action occurred in this District, Defendant operates retail locations within this District, and the Data Breach affected consumers in this District.

FACTUAL BACKGROUND

DEFENDANT'S COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION AND PAYMENT CARD DATA

9. Defendant is an American luxury specialty department store. Millions of Americans regularly shop at Defendant's online and brick-and-mortar stores.

10. When individuals transact business with Defendant or visit one of its stores or website, Defendant collects a wide variety of PII about them.

11. Defendant discloses the Information it collects about individuals who either shop online or in stores – or simply enter any of its stores or browse its website, even without making a purchase – on its website:

> **The Information We Collect**
>
> Generally, you may browse the website without providing any personally identifiable information. However, we may ask you to provide personally identifiable information at various times and places on this website. In some cases, if you choose not to provide us with the requested information, you may not be able to access all of this website or participate in all of its features.
>
> We receive and store any personally identifiable information you enter on the website, whenever you shop with Neiman Marcus—online, through our catalogs, or in our stores, or information you give us in any other way, such as by subscribing to our catalogs, email, or mobile messaging. **For example, we may collect the**

following personally identifiable information: your name, address, telephone number, mobile telephone number, driver's license number, birth date, and email address. If you use a credit or debit card or pay by check, we will also include your account number.

When you register with us as an online customer, we may ask for additional information, such as your favorite designers.

If you use one of our services, or participate in one of our surveys, promotions, or sweepstakes, we may ask for additional information, such as **your age, interests, or product preferences**.

From your purchases and other interactions with us, we obtain information concerning the specific products or services you purchase or use.

When you visit this website, our web server automatically collects anonymous information such as log data and IP addresses, and may collect general information concerning your location. We may use the automatically collected information for a number of purposes, such as improving our site design, product assortments, customer service, and special promotions.

When you visit one of our stores, if your mobile device accesses one of our wireless networks we may also automatically collect information about your geo-location based, in part, upon which wireless network has been accessed. When this happens **we attempt** to de-identify the information, which means that we remove or change (e.g., hash) certain pieces of information that might be used to link the data to you, or to your device. We will not attempt to re-identify geo-location information (i.e., link it to you or your device) unless you affirmatively give us permission to collect geo-location information about you. If you give us such permission, you can later decide to opt-out of geo-location tracking by sending an email to geo_optout@neimanmarcus.com with your MAC address (which can be found on most mobile devices under the "settings" menu).

Our mobile applications will not transmit geo-location information about you to us unless you give them permission to do so.

Some web browsers and devices permit you to broadcast a preference that you not be "tracked" online. **At this time we do**

> **not modify your experience based upon whether such a signal is broadcast**.

<http://www.neimanmarcus.com/assistance/assistance.jsp?itemId=cat33940739 (Security & Privacy Tab, "Information We Collect" last updated December 17, 2013)> (emphasis added) (last visited Feb. 28, 2014).

12. Thus, Defendant stores massive amounts of PII on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

IMPORTANCE OF DATA SECURITY TO PURCHASING DECISIONS

13. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiffs would not have made purchases at Neiman Marcus, or would not have paid as much for them, had they known that Neiman Marcus does not take all necessary precautions to secure their personal and financial data. Neiman Marcus failed to disclose its negligent and insufficient data security practices and consumers relied on this omission to make purchases at Neiman Marcus.

14. Furthermore, when consumers purchase goods at a high-end retailer, such as Defendant, they assume that its data security practices and policies are state of the art and that the retailer will use part of the purchase price that consumers to pay for such state of the art practices. Consumers thus enter into an implied contract with Defendant that Defendant will adequately secure and protect their Private Information, and will use part of the purchase price of the goods to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, Neiman Marcus simply kept the money to maximize its profits, thus breaching the implied contract.

VALUE OF PII TO COMPANIES AND HACKERS

15. A market exists for personal data and information regarding individuals' preferences and interests. This information is valuable because it can be compiled and sold as demographic data and advertising analytics or sold on a per-name basis. Companies like infoUSA compile consumer information and sell name and contact information categorized by demographic data, interests or other behavioral information.

16. It is well known and the subject of many media reports that PII data is also highly coveted by and a frequent target of hackers. PII data is often easily taken because it is less protected and regulated than PCD.

17. Thus, both legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't pay for it or aggressively seek it. For example, in "[o]ne of 2013's largest breaches . . . [n]ot only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users . . . ." Verizon 2014 PCI Compliance Report, <http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf>(hereafter "2014 Verizon Report"), at 54. Similarly, in the Target data breach, in addition to PCD pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

18. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. Unfortunately, and as will be alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as retailers, Defendant's approach at maintaining the security

of Plaintiffs' and Class Members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

LACK OF SEGREGATION OF CARD HOLDER DATA FROM PII

19. Unlike PII data, payment card data is heavily regulated. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

20. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data." PCI DSS v. 2 at 5 (2010) ("PCI Version 2").

21. PCI Version 2.0 prohibits retailers such as Defendant from: (1) improperly storing and retaining credit card transaction and customer data in an unencrypted, unsecure, and unauthorized manner; (2) failing to render PCD on electronic media unrecoverable so that it cannot be reconstructed; (3) failing to properly install, implement and maintain firewall(s) to protect consumer data; (4) failing to properly limit inbound Internet traffic to certain IP addresses; (5) failing to perform dynamic packet filtering; (6) failing to properly restrict access to the business's computers; (7) failing to properly protect stored data; (8) failing to encrypt cardholder data and other sensitive information; (9) failing to properly use and regularly update anti-virus software or programs; (10) failing to track and monitor all access to network resources and cardholder data; and (11) failing to regularly test security systems or run vulnerability scans at least quarterly and after any significant network change.

22. One critical PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date,

and Service Code. *Id*. at 7.

23. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement." *Id*. at 10. However, segregation is recommended because among other reasons, "[i]t's not just cardholder data that's important; criminals are also after other personally identifiable information (PII) and corporate data." *See* Verizon Report at 54.

24. Many state statutes mandate additional data security requirements. For example, Cal. Civil Code § 1798.81 requires businesses to "take all reasonable steps to dispose, or arrange for the disposal, of customer records within [their] custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."

25. Illicitly obtained PII and PCD is sold on the black market, including on websites, as a product at a set price. *See, e.g.*, <http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth> (last visited Mar. 4, 2014).

THE DATA BREACH AFFECTING NEIMAN MARCUS

26. Defendant's credit card processor, TSYS, notified Defendant on December 13, 2013 that fraudulent card usage had been linked to a "common point of purchase" at Neiman Marcus stores. Visa and Mastercard confirmed additional fraud over the next few days. <http://online.wsj.com/news/articles/SB10001424052702303947904579338570638774960> (last visited Mar. 12, 2014).

27. Nevertheless, Defendant waited until news of the Data Breach was first published by a blogger (Brian Krebs of <http://krebsonsecurity.com/>) on or about January 10, 2014, some twenty-eight (28) days later, before making any attempt whatsoever to notify affected customers.

28. On January 10, 2014, instead of notifying affected customers directly, Defendant posted a statement on its Twitter account (not on the shopping site regularly accessed by customers), vaguely indicating: "The security of our customers' information is always a priority and we sincerely regret any inconvenience"; and "We are taking steps, where possible, to notify customers whose cards we know were used fraudulently after purchasing at our stores." <https://twitter.com/neimanmarcus> (last visited Jan. 12, 2014).

29. On January 12, 2014, Ginger Reeder, a spokeswoman for Defendant, confirmed that Defendant "had been notified in mid-December by its credit card processor about potentially unauthorized payment activity following customer purchases at stores." <http://abcnews.go.com/US/wireStory/neiman-marcus-victim-cyber-security-attack-21498673> (last visited Jan. 12, 2014).

30. The malware that was capable of collecting Payment Card data and that a hacker or hackers successfully inserted into Neiman Marcus's system is referred to as the "Malware," herein.

31. During the months that hackers were scouring Defendant's information systems, 59,746 alerts were set off by malware indicating "suspicious behavior" within Defendant's security system. *Id.* However, Defendant's centralized security system's ability to automatically block the activity was "turned off." *Id.* Defendant has failed to

explain why it ignored nearly 60,000 alerts that should have led it to discover and stop the Data Breach.

32. On information and belief, the Malware operated in Defendant's stores at physical locations operating under the "Neiman Marcus," "Bergdorf Goodman," "Cusp," and "Last Call" names ("NMG Stores") between July 16, 2013 to and October 30, 2013 ("the Malware Period").

33. On information and belief, however, the Malware never operated in some NMG Stores, and never operated in any restaurants owned by Neiman Marcus or on any website or online store.

34. On information and belief, as to the NMG Stores where the Malware did operate, it did not operate in each of the stores during each day of the Malware Period but instead operated on dates that varied from store to store.

35. On information and belief, at times the Malware only operated during part of the time that an affected NMG Store was open for business, and the times when the Malware operated varied from day to day within each individual NMG Store and among the NMG Stores where the Malware operated.

36. On information and belief, during the Malware Period, approximately 1,144,827 different Payment Card accounts were used at NMG Stores. Out of these approximately 1,144,827 different Payment Card accounts, approximately 370,385 Payment Card accounts were used at a NMG Store during the Malware Period on a date and at a time that the Malware was operating in that store. The remaining approximately 774,442 Payment Card accounts were not exposed to the Malware at any time and could not have been compromised as a result of the Cybersecurity Incident.

37. Hacking is often accomplished in a series of phases to include reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining access, escalation of user, computer and network privileges, maintaining access, covering tracks and placing backdoors.

38. The malware as described by Defendant does not appear to have initiated or caused the infiltration into Defendant's system or networks. Instead, this malware appears to have come later in order to maintain control of the system, execute programs or processes and to parse and syphon consumer confidential data.

39. On information and belief, Defendant failed to properly segregate PII from payment card data. As a result, while hackers scoured Defendant's networks to find a way into the point-of-sale ("POS"), they had access to and collected PII stored on Defendant's networks.

CONSEQUENCES OF DEFENDANT'S CONDUCT

40. According to Defendant, 370,385 credit and debit cards swiped in 77 U.S. stores were affected by the Data Breach in 2013, including "Last Call" outlets.

41. According to Defendant, "approximately 9,200 of those [credit or debit cards used at its stores] were subsequently used fraudulently elsewhere." <http://www.neimanmarcus.com/en-au/NM/Security-Info/cat49570732/c.cat?icid=topPromo_hmpg_ticker_SecurityInfo_0114> (last visited Mar. 5, 2014).

42. On information and belief, Plaintiff Remijas's identifying and/or financial information was disclosed in the Data Breach. On information and belief, Plaintiff Kao's identifying and/or financial information was not disclosed in the Data Breach, although she shopped during the Malware Period.

43.

44. Defendant failed to provide reasonable and appropriate security for the PII and PCD that it collected and maintained.

45. The ramifications of Defendant's failure to keep Class members' data secure are severe.

46. The information Defendant lost, including Plaintiffs' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC Interactive Toolkit, *Fighting Back Against Identity Theft*, available at <http://www.vanderbilt.edu/PersonalIdentityTheftProtection.pdf > (last visited Mar. 12, 2014). Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. *Id.*

47. As the FTC has stated, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." FTC, Signs of Identity Theft, available at <http://www.consumer.ftc.gov/articles/0271-signs-identity-theft> (last visited Jan. 21, 2014).

48. According to Javelin Strategy and Research, "one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year." <http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identity-

theft-victim-every-2-seconds-last-year>.

49. Identity thieves can use personal information such as that pertaining to the Class, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. This activity may not come to light for years.

50. In addition, identity thieves may get medical services using consumers' lost information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

51. It is incorrect to assume that reimbursing a consumer for fraud makes that individual whole again. On the contrary, after conducting a study the Department of Justice's Bureau of Justice Statistics ("BJS") found that "[a]mong victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." Victims of Identity Theft, 2012 at 1 (2013), available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Mar. 5, 2014). In fact, the BJS reported, "[r]esolving the problems caused by identity theft [could] take more than a year for some victims." *Id.* at 11.

52. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [S]tolen 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.

GAO, *Report to Congressional Requesters*, at p. 29 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf>.

53. Given that at least 9,200 confirmed instances of fraud have already resulted from the Data Breach to date, Plaintiffs and the Class they seek to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them, and the resulting loss of use of their credit and access to funds whether or not such charges are ultimately reimbursed by the credit card companies.

54. Plaintiffs would not have shopped at Defendant's stores, paid as much for the products they purchased there, or visited Defendant's stores or website, had they known that Defendant would not adequately protect their personal and financial information.

CLASS ACTION ALLEGATIONS

55. Plaintiffs seek relief in their individual capacity and seek to represent a class consisting of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiffs seek certification of a class initially defined as follows:

> All residents of the United States who held a credit card or debit card account that was used in any NMG Store during the Malware Period. Excluded from the Settlement Class are the judge presiding over this matter, any members of his judicial staff, the officers and directors of Neiman Marcus.

56. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of

Class members is unknown to Plaintiffs at this time, approximately 1,144,827 different payment cards were used during the Malware Period, indicating that there are hundreds of thousands, or potentially over one million, class members.

57. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost or disclosed Class members' personal and/or financial information;

b. Whether Defendant unreasonably delayed in notifying affected customers of the Data Breach and whether the belated notice was adequate;

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

d. Whether Defendant's conduct was negligent;

e. Whether Defendant's conduct violated New York General Business Law § 349;

f. Whether Defendant's conduct violated 815 ILCS 505/1;

g. Whether Defendant entered into an implied contract with Plaintiffs and Class Members containing a term to safeguard their Private Information;

h. Whether Defendant violated the requirements of California Civil Code § 1798.80 *et seq.*;

i. Whether Defendant's conduct violated California Business & Professions

Code § 17200, *et seq.*;

j. Whether Defendant's conduct constituted conversion under California law;

k. Whether Defendant breached its bailment duty under California law;

l. Whether Defendant acted willfully and/or with oppression, fraud, or malice;

m. Whether Defendant's conduct constituted Intrusion under California law;

n. Whether Defendant's conduct constituted Public Disclosure of Private Facts under California law;

o. Whether Defendant's conduct constituted Misappropriation of Likeness and Identity under California law;

p. Whether Defendant's conduct violated Class members' California Constitutional Right to Privacy;

q. Whether Defendant willfully and/or negligently violated the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*; and

r. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

58. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiffs held a credit card or debit card account that was used in a NMG Store during the Malware Period.

59. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

60. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

61. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

62. Defendant has acted or refused to act on grounds that apply generally to the class, as alleged above, and certification is proper under Rule 23(b)(2).

FIRST COUNT

Negligence
(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)

63. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

64. Plaintiffs bring this claim individually and on behalf of the nationwide Class.

65. Defendant knowingly collected, came into possession of and maintained Plaintiffs' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

66. Defendant had and continues to have a duty to timely disclose that

Plaintiffs' Private Information within its possession might have been compromised and precisely the types of information that were compromised.

67. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' Private Information.

68. Defendant systematically failed to provide adequate security for data in its possession.

69. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' Private Information within Defendant's possession.

70. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' Private Information.

71. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class members the fact that their Private Information within its possession might have been compromised and precisely the type of information compromised.

72. Defendant's breach of duties owed to Plaintiffs and the Class proximately caused Plaintiffs' and Class members' Private Information to be compromised.

73. As a result of Defendant's ongoing failure to notify consumers regarding what type of PII has been compromised, consumers are unable to take the necessary precautions to mitigate their damages by preventing future fraud.

74. Defendant's breaches of duty caused Plaintiffs to overpay for goods, purchase goods they would not otherwise have purchased, suffer fraud on their credit or

debit cards, identity theft, phishing, temporary loss of use of their debit cards and access to the funds therein, loss of time and money associated with resolving the fraudulent charges on their cards, loss of time to monitor and cancel additional cards or accounts, loss of time and money monitoring their finances for additional fraud, diminished value of the services they received, and loss of control over their PCD and/or PII.

75. As a result of Defendant's negligence and breach of duties, Plaintiff Remijas's Private Information was compromised and obtained by a third party.

76. Additionally, Plaintiff Remijas is in danger of imminent harm that her PII, which is still in the possession of third parties, will be used for fraudulent purposes.

77. Plaintiffs seek the award of actual damages on behalf of the Class.

78. In failing to secure Plaintiffs' and Class members' Private Information and promptly notifying them of the Data Breach, Defendant was guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

79.

SECOND COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)

80. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

81. Defendant required customers who intended to make In Store Purchases with debit or credit cards to provide their cards' magnetic strip data for payment verification.

82. In providing such information, Plaintiffs and other Class members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard their sensitive and non-public information.

83. Defendant breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard their financial data. Plaintiffs and Class Members suffered and will continue to suffer damages including, but not limited to, actual identity theft, fraud and/or phishing, loss of money and costs incurred as a result of increased risk of identity theft, and loss of their PCD and PII, all of which have ascertainable value to be proved at trial.

THIRD COUNT

Unjust Enrichment
(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)

84. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein

85. Plaintiffs hereby plead in the alternative to the Second Count.

86. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiffs and the Class.

87. Defendant appreciates or has knowledge of such benefit.

88. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class members, which Defendant has unjustly received as a result of its unlawful actions.

89. As a result of Defendant's conduct, Plaintiffs and the Class suffered and will continue to suffer actual damages including, but not limited to, the release of their Private Information; expenses and/or time spent on credit monitoring and identity theft insurance;

time spent scrutinizing bank statements, credit card statements, and credit reports; and, time spent initiating fraud alerts. Plaintiffs and Class members suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, other economic and non-economic losses.

FOURTH COUNT

Unfair and Deceptive Business Practices

(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)

90. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

91. Plaintiffs bring this Count individually, and on behalf of all similarly situated residents of each of the 50 States and the District of Columbia, for violations of the respective statutory consumer protection laws, as follows:

a. the Alabama Deceptive Trade Practices Act, Ala.Code 1975, § 8–19–1, *et seq*.

b. the Alaska Unfair Trade Practices and Consumer Protection Act, AS § 45.50.471, *et seq*.;

c. the Arizona Consumer Fraud Act, A.R.S §§ 44-1521, *et seq*.;

d. the Arkansas Deceptive Trade Practices Act, Ark.Code §§ 4-88-101, *et seq*.;

e. the California Unfair Competition Law, Bus. & Prof. Code §§17200, *et seq*. and 17500 *et seq*.;

f. the California Consumers Legal Remedies Act, Civil Code §1750, *et seq*.;

g. the Colorado Consumer Protection Act, C.R.S.A. §6-1-101, *et seq*.;

h. the Connecticut Unfair Trade Practices Act, C.G.S.A. § 42-110, *et seq*.;

i. the Delaware Consumer Fraud Act, 6 Del. C. § 2513, *et seq*.;

j. the D.C. Consumer Protection Procedures Act, DC Code § 28-3901, *et seq*.;

k. the Florida Deceptive and Unfair Trade Practices Act, FSA § 501.201, *et seq*.;

l. the Georgia Fair Business Practices Act, OCGA § 10-1-390, *et seq*.;

m. the Hawaii Unfair Competition Law, H.R.S. § 480-1, *et seq*.;

n. the Idaho Consumer Protection Act, I.C. § 48-601, *et seq*.;

o. the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1 *et seq*.;

p. the Indiana Deceptive Consumer Sales Act, IN ST § 24-5-0.5-2, *et seq*.

q. The Iowa Private Right of Action for Consumer Frauds Act, Iowa Code Ann. § 714H.1, *et seq*.;

r. the Kansas Consumer Protection Act, K.S.A. § 50-623, *et seq*.;

s. the Kentucky Consumer Protection Act, KRS 367.110, *et seq*.;

t. the Louisiana Unfair Trade Practices and Consumer Protection Law, LSA-R.S. 51:1401, *et seq*.;

u. the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A, *et seq*.;

v. the Maryland Consumer Protection Act, MD Code, Commercial Law, § 13-301, *et seq*.;

w. the Massachusetts Regulation of Business Practices for Consumers Protection Act, M.G.L.A. 93A, *et seq*.;

x. the Michigan Consumer Protection Act, M.C.L.A. 445.901, *et seq*.;

y. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F.68, *et seq*.;

z. the Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq*.

aa. the Missouri Merchandising Practices Act, V.A.M.S. § 407, *et seq*.;

bb. the Montana Unfair Trade Practices and Consumer Protection Act of 1973, Mont. Code Ann. § 30-14-101, *et seq*.;

cc. the Nebraska Consumer Protection Act, Neb.Rev.St. §§ 59-1601, *et seq*.;

dd. the Nevada Deceptive Trade Practices Act, N.R.S. 41.600, *et seq*.

ee. the New Hampshire Regulation of Business Practices for Consumer Protection, N.H.Rev.Stat. § 358-A:1, *et seq*.;

ff. the New Jersey Consumer Fraud Act, N.J.S.A. 56:8, *et seq*.;

gg. the New Mexico Unfair Practices Act, N.M.S.A. §§ 57-12-1, *et seq*.;

hh. the New York Consumer Protection from Deceptive Acts and Practices, N.Y. GBL (McKinney) § 349, *et seq.*;

ii. the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, *et seq*.;

jj. the North Dakota Consumer Fraud Act, N.D. Cent.Code Chapter 51-15, *et seq*.;

kk. the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq*.;

ll. the Oklahoma Consumer Protection Act, 15 O.S.2001, §§ 751, *et seq*.;

mm. the Oregon Unlawful Trade Practices Act, ORS 646.605, *et seq*.;

nn. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq*.;

oo. the Rhode Island Deceptive Trade Practices Act, G.L.1956 § 6-13.1-5.2(B), *et seq*.;

pp. the South Carolina Unfair Trade Practices Act, SC Code 1976, §§ 39-5-10, *et seq*.;

qq. the South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, *et seq*.;

rr. the Tennessee Consumer Protection Act, T.C.A. § 47-18-101, *et seq*.;

ss. the Texas Deceptive Trade Practices-Consumer Protection Act, V.T.C.A., Bus. & C. § 17.41, *et seq*.;

tt. the Utah Consumer Sales Practices Act, UT ST § 13-11-1, *et seq*.;

uu. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, *et seq*.;

vv. the Virginia Consumer Protection Act of 1977, VA ST § 59.1-196, *et seq*.;

ww. the Washington Consumer Protection Act, RCWA 19.86.010, *et seq*.;

xx. the West Virginia Consumer Credit And Protection Act, W.Va.Code § 46A-1-101, *et seq*.;

yy. the Wisconsin Deceptive Trade Practices Act, WIS.STAT. § 100.18, *et seq*.; and

zz. the Wyoming Consumer Protection Act, WY ST § 40-12-101, *et seq*.

92. Defendant violated the statutes set forth (collectively, the "Consumer Protection Acts") above by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs and Class Members' PII, and by allowing third parties to access Plaintiffs' and Class Members' PII.

93. Defendant further violated the Consumer Protection Acts by failing to disclose to the consumers that its data security practices were inadequate, thus inducing consumers to make purchases at Neiman Marcus.

94. Defendant's acts and/or omissions constitute fraudulent, deceptive, and/or unfair acts or omissions under the Consumer Protection Acts.

95. Plaintiffs and other Class Members were deceived by Defendant's failure to properly implement adequate, commercially reasonable security measures to protect their PII.

96. Defendant intended for Plaintiffs and other Class Members to rely on Defendant to protect the information furnished to it in connection with debit and credit

card transactions and/or otherwise collected by Defendant, in such manner that Plaintiffs' PII would be protected, secure and not susceptible to access from unauthorized third parties.

97. Defendant instead handled Plaintiffs' and other Class Members' information in such manner that it was compromised.

98. Defendant failed to follow industry best practices concerning data security or was negligent in preventing the Data Breach from occurring.

99. It was foreseeable that Defendant's willful indifference or negligent course of conduct in handling PII it collected would put that information at the risk of compromise by data thieves.

100. On information and belief, Defendant benefited from mishandling the PII of customers, In Store Visitors and Online Shoppers because, by not taking effective measures to secure this information, Defendant saved on the cost of providing data security.

101. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiffs' and Class Members' reliance on Defendant's deception that their Private Information was secure.

102. Defendant's conduct offends public policy and constitutes unfair acts or practices under the Consumer Protection Acts because Defendant caused substantial injury to Class Members that is not offset by countervailing benefits to consumers or competition, and is not reasonably avoidable by consumers.

103. Defendant's acts or practice of failing to employ reasonable and appropriate security measures to protect Private Information constitute violations of the

Federal Trade Commission Act, 15 U.S.C. § 45(a), which the courts consider when evaluating claims under the Consumer Protection Acts, including 815 ILCS 505/2.

104. Defendant's conduct constitutes unfair acts or practices as defined in the Consumer Protection Acts because Defendant caused substantial injury to Class members, which injury is not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

105. Defendant also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et. seq*., which provides, at Section 10:

> Notice of Breach.
>
> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

106. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

107. Plaintiffs and other Class Members have suffered injury in fact and actual damages including lost money and property as a result of Defendant's violations of the Consumer Protection Acts.

108. Defendant's fraudulent and deceptive behavior proximately caused Plaintiffs' and Class Members' injuries, and Defendant conducted itself with reckless

indifference toward the rights of others, such that an award of punitive damages is appropriate.

109. Defendant violated the Consumer Protection Acts, which laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

110. Defendant's failure to disclose information concerning the Data Breach directly and promptly to affected customers, constitutes a separate fraudulent act or practice in violation of the Consumer Protection Acts, including California Business & Professions Code § 17200, *et seq*.

111. Plaintiffs seek restitution pursuant to the Consumer Protection Acts, including California Business & Professions Code § 17203, and injunctive relief on behalf of the Class.

112. Plaintiffs seek attorney's fees and damages to the fullest extent permitted under the Consumer Protection Acts, including N.Y. G.B.L. § 349(h).

FIFTH COUNT

Invasion of Privacy - Intrusion, Public Disclosure of Private Facts, Misappropriation of Likeness and Identity, and California Constitutional Right to Privacy
(On Behalf of Plaintiff Kao and All Other Similarly Situated California Consumers)

113. Plaintiff Kao incorporates the substantive allegations contained in all previous paragraphs as if fully set forth herein.

114. Plaintiff Kao and other California class members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

115. By failing to keep California class members' Private Information safe, and by

misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded California class members' privacy by:

a. Intruding into California class members' private affairs in a manner that would be highly offensive to a reasonable person;

b. Publicizing private facts about California class members, which is highly offensive to a reasonable person;

c. Using and appropriating California class members' identity without her consent; and

d. Violating California class members' right to privacy under California Constitution, Article 1, Section 1, through the improper use of their Private Information properly obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

116. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in California class members' position would consider Defendant's actions highly offensive.

117. Defendant invaded California class members' right to privacy and intruded into her and other California class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

118. As a proximate result of such misuse and disclosures, California class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of California class members' protected privacy interests.

119. In failing to protect California class members' Private Information, and in

misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of California class members' and the Class Members' rights to have such information kept confidential and private. The California class members, therefore, seek an award of damages, including punitive damages, on behalf of themselves and the Class.

SIXTH COUNT
Violation of State Data Breach Acts
(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)

120. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

121. Defendant owns, licenses and/or maintains computerized data that includes Plaintiffs' and Class Members' PII.

122. Defendant was required to, but failed, to take all reasonable steps to dispose, or arrange for the disposal, of records within its custody or control containing personal information when the records were no longer to be retained, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

123. Defendant's conduct, as alleged above, violated the data breach statutes of many states, including:

a. California, Cal. Civ. Code §§ 1798.80 *et. seq*.;

b. Hawaii, Haw. Rev. Stat. § 487N-1–4 (2006);

c. Illinois, 815 Ill. Comp Stat. Ann. 530/1–/30 (2006);

d. Louisiana, La. Rev. Stat. § 51:3071-3077 (2005), and L.A.C. 16:III.701;

e. Michigan, Mich. Comp. Laws Ann. §§ 445.63, 445.65, 445.72 (2006);

f. New Hampshire, N.H. Rev. Stat. Ann. §§ 359-C:19–C:21, 358-A:4 (2006)., 332-I:1–I:610;

g. New Jersey, N.J. Stat. Ann. § 56:8-163–66 (2005);

h. North Carolina, N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009);

i. Oregon, Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624 (2011);

j. Puerto Rico, 10 L.P.R.A. § 4051; 10 L.P.R.A. § 4052 (2005), as amended (2008);

k. South Carolina, S.C. Code § 1-11-490 (2008); S.C. Code § 39-1-90 (2009);

l. Virgin Islands, 14 V.I.C. § 2208, et seq. (2005);

m. Virginia, Va. Code Ann. § 18.2-186.6 (2008); Va. Code Ann. § 32.1– 127.1:05 (2011); and

n. the District of Columbia, D.C. Code § 28-3851 to 28-3853 (2007) (collectively, the "State Data Breach Acts").

124. Defendant was required to, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

125. The Data Breach constituted a "breach of the security system" within the meaning of section 1798.82(g) of the California Civil Code, and other State Data Breach Acts.

126. The information compromised in the Data Breach constituted "personal information" within the meaning of section 1798.80(e) of the California Civil Code, and other State Data Breach Acts.

127. Like other State Data Breach Acts, California Civil Code § 1798.80(e) requires disclosure of data breaches "in the most expedient time possible and without unreasonable

delay . . . ."

128. Defendant violated Cal. Civ. Code § 1798.80(e) and other State Data Breach Acts by unreasonably delaying disclosure of the Data Breach to Plaintiffs and other Class Members, whose PII was, or was reasonably believed to have been, acquired by an unauthorized person.

129. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiffs and Class Members would impede a criminal investigation.

130. As a result of Defendant's violation of State Data Breach Acts, including Cal. Civ. Code § 1798.80, *et seq.*, Plaintiffs and Class Members incurred economic damages, including expenses associated with monitoring their personal and financial information to prevent further fraud.

131. Plaintiffs, individually and on behalf of the Class, seek all remedies available under Cal. Civ. Code § 1798.84 and under the other State Data Breach Acts, including, but not limited to: (a) actual damages suffered by Class Members as alleged above; (b) statutory damages for Defendant's willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; (c) equitable relief; and (d) reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

132. Because Defendant was guilty of oppression, fraud or malice, in that it failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights, Plaintiffs also seek punitive damages, individually and on behalf of the Class.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs

and their Counsel to represent the Class;

B. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

C. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

D. For an award of punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

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

Dated: October 15, 2019

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson

Tina Wolfson, (*pro hac vice* application granted)
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: (310) 474-9111
Fax: (310) 474-8585

Joseph J. Siprut
Bruce Howard
SIPRUT PC
17 North State Street, Suite 1600
Chicago, IL 60602
Tel: (312) 236-0000
Fax: (312) 267-1906

John A. Yanchunis, Sr., (*pro hac vice* application to be filed)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
Fax: (813) 223-5402

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

The undersigned, an attorney, hereby certifies that a true and correct copy of the foregoing document was filed electronically with the Clerk of the Court using the CM/ECF system on October 15, 2019, and served electronically on all counsel of record.

/s/ Tina Wolfson
Tina Wolfson