IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

ANDREW MCCLEASE, on behalf of himself and all others similarly situated,	)	
Plaintiff,	)	Civil Action No.:
v.	)	CLASS ACTION COMPLAINT JURY TRIAL DEMANDED
THE NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company	)	
Defendant.	)	

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff, ANDREW MCCLEASE, by and through the undersigned attorneys, brings this Class Action Complaint against the Defendant, NEIMAN MARCUS GROUP, LLC (hereafter referred to as "Neiman" or "Defendant") and alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings 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 Plaintiff 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, Plaintiff brings this action against Defendant asserting claims for negligence, violation of North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, *et seq.*; and violation of the Fair Credit Reporting Act, codified at 15 U.S.C. § 1681 *et. seq.*

PARTIES

3. Plaintiff Andrew McClease is a current resident of Manteo, which lies in Dare County, North Carolina. Mr. McClease made purchases using a Neiman Marcus charge card at a Neiman Marcus location in Charlotte, North Carolina, in April, 2013, and again in December 2013. Mr. McClease received notice from Defendant about the Data Breach in March 2014. Hackers stole Mr. McClease's data and used his card fraudulently. While the charges were reversed, Mr. McClease paid interest on the fraudulent charges for which he was not compensated.

4. Defendant The Neiman Marcus Group, LLC ("Defendant") is a Delaware limited liability company headquartered in Dallas, Texas. Defendant operates retail stores throughout the United States, including on Sharon Road in Charlotte, located in Mecklenburg County, North Carolina. 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

5. 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.

6. This Court has personal jurisdiction over Defendant because Defendant is authorized to and does conduct substantial business in North Carolina, and in this District. Defendant owns and operates retail locations in the state of North Carolina.

7. 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 in North Carolina, and the Data Breach affected consumers in this District.

FACTUAL BACKGROUND

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

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

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

10. 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).

11. 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

12. 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.

13. 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

14. 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.

15. 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.

16. 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.

17. 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

18. 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.

19. "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").

20. 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.

21. 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.

22. "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.

23. 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."

24. Illicitly obtained PII and PCD is sold on the black market, including on websites, as a product at a set price.[1]

THE DATA BREACH AFFECTING NEIMAN MARCUS

25. 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.[2] Nevertheless, Defendant waited until news of the Data Breach was first published by

[1] Krebs on Security, *How Much is Your Identity Worth?*, Nov. 11, 2013, available at http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/ (last visited Nov. 14, 2014).

[2] *See* Suzanne Kapner, *Malware Lurked for Months Inside Neiman*, Wall St. J., Jan. 23, 2014, available at http://online.wsj.com/news/articles/SB10001424052702303947904579338570638774960 (last visited Nov. 14, 2014).

blogger Brian Krebs of Krebs On Security on or about January 10, 2014, some twenty-eight (28) days later, before making any attempt whatsoever to notify affected customers.

26. 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."

27. 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.". Ms. Reeder "wouldn't estimate how many customers may [have] be affected but said the merchant [wa]s notifying customers whose cards it ha[d] now determined were used fraudulently."

28. While Defendant has stated that "there is no indication that" social security numbers, PINs and dates of birth were compromised, it has not disclosed whether the wide range of other PII that it collects, including names, addresses, telephone numbers, mobile telephone numbers, driver's license numbers, bank account numbers, email addresses, computer IP addresses, and location information, were disclosed in the breach. Without such detailed disclosure, Plaintiffs and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

29. Moreover, while Defendant claims that card data was scraped between July

16 and October 30, 2013, it acknowledges that "[o]ther malware associated with the attack, but not capable of scraping card data, was found to be in the environment as early as March." Defendant has failed to disclose the effects of this "other malware" and whether or not and when this malware was extinguished.

30. It's very unusual for malware to self-expire. In addition, if fraud were occurring between July and October 2013, because hackers already had their hands on cardholder data and PII, credit card company analytics and other methods (undercover investigations of the black market) would likely have discovered it before December of 2013. Defendant has failed to provide a cogent picture of how the Data Breach occurred and its full effects on customers' PII and PCD.

31. Reports further state that "hackers took control of a vulnerable server" which connected both to Defendant's secure payment system and its general purpose network. This lack of segregation suggests that hackers had access to both PCD and PII during the Breach. *See* <http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data>.

32. 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 sixty thousand alerts that should have led it to discover and stop the Data Breach.

33. 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.

34. 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.

35. 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.

36. On information and belief, the Data Breach lasted for a longer time period than July 16-October 30, 2013. On information and belief, the Data Breach began no later than March 2013 when hackers took control of "a vulnerable server" belonging to Defendant, and lasted until January 10, 2014, when the Data Breach was finally contained.

CONSEQUENCES OF DEFENDANT'S CONDUCT

37. According to Defendant, 350,000 credit and debit cards swiped in 77 U.S. stores were affected by the Data Breach in 2013, including "Last Call" outlets.

38. According to Defendant, "approximately 9,200 of those [credit or debit cards used at its stores] were subsequently used fraudulently elsewhere."[3]

39. Plaintiff's identifying and/or financial information was disclosed in the Data Breach.

[3] Statement of Karen Katz, President and CEO of Neiman Marcus, *To our Loyal Neiman Marcus Group Customers*, June 15, 2014, available at http://www.neimanmarcus.com/NM/Security-Info/cat49570732/c.cat (last visited Nov. 14, 2014).

40. Plaintiff Andrew McClease had never suffered any type of fraud, or identity theft before the Data Breach.

41. On or about April or May 2014, an unauthorized charge of $450 appeared on Plaintiff's Neiman charge card from a store in Boston, Massachusetts.

42. The above unauthorized charge was not removed from Plaintiff's charge card until June or July 2014, and Plaintiff paid interest on the charge during the intervening period.

43. On information and belief, the fraudulent charges on Plaintiff's charge card were fairly traceable to Defendant's negligence and its failure to keep Plaintiff's personal and/or financial information secure.

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. Plaintiff's experience here confirms the veracity of the BJS statistics detailed above. For example, while the last purchase using his charge account was made at Defendant's store in December 2013, he did not suffer fraud on his Neiman charge card until the following April or May 2014.

53. 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>. Plaintiff's experience corroborates GAO's finding that there may be, and often is, a time lag between when harm occurs versus when it is discovered, and also between when PII or payment card data is stolen and when it is used.

54. Given that at least 9,200 confirmed instances of fraud have already resulted from the Data Breach to date, Plaintiff and the Class they seeks 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.

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

CLASS ACTION ALLEGATIONS

56. Plaintiff seeks relief in his individual capacity and seeks 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), Plaintiff seeks certification of a class initially defined as follows:

> All persons whose personal and/or financial information was disclosed in the data incursion affecting Neiman Marcus in 2013. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

57. 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, based on information and belief, it is in the millions.

58. 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 various state consumer protection and business laws;

f. Class Members containing a term to safeguard their Private Information;

g. Whether Defendant's conduct constituted Misappropriation of Likeness and Identity under relevant state laws;

h. Whether Defendant's conduct violated Class members' Right to Privacy;

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

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

59. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by Defendant.

60. 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.

61. 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.

62. 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.

63. 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 Plaintiff and All Other Similarly Situated United States Consumers)

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

65. Plaintiff brings this claim individually and on behalf of the nationwide Class.

66. Defendant knowingly collected, came into possession of and maintained Plaintiff's 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.

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

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

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

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

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

71. 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.

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

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

74. 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.

75. Defendant's breaches of duty caused Plaintiff 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.

76. As a result of Defendant's negligence and breach of duties, Plaintiff's and Class Members' Private Information was compromised, obtained by a third party, and used by a third party to cause Plaintiff to incur fraudulent charges, to spend time clearing up those charges, and to pay interest on those charges until they were removed from his charge account.

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

78. Plaintiff seeks the award of actual damages on behalf of the Class.

79. In failing to secure Plaintiff's 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.

80. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII have been compromised as a result of the data breach.

SECOND COUNT

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

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

82. 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.

83. 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.

84. 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 identity theft and/or the 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)

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

86. Plaintiff hereby pleads in the alternative to the Second Count.

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

88. Defendant appreciates or has knowledge of such benefit.

89. 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.

90. 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)

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

92. Plaintiff brings 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*.

93. 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.

94. Defendant further violated the Consumer Protection Acts, including the

North Carolina Unfair and Deceptive Trade Practices Act, by failing to disclose to the consumers that its data security practices were inadequate, thus inducing consumers to make purchases at Neiman Marcus.

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

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

97. 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.

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

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

100. 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.

101. 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.

102. 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.

103. 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.

104. 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 the North Carolina Unfair and Deceptive Trade Practices Act (UDTPA).

105. Defendant further violated UDTPA by violating the Identity North Carolina's Identity Theft Protection Act (ITPA), N.C.G.S. § 75-60, *et. seq*. (ITPA).

106. Defendant violated ITPA by:

a. Failing to prevent the personal information of customers from falling into unauthorized hands;

b. Failing to properly dispose of all personal information of their customers; and,

c. Failing to provide adequate notice of the security breach to affected consumers upon discovery that their system had been compromised and personal information had been stolen.

107. 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.

108. Plaintiff 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.

109. 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.

110. 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.

111. 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.

112. The California Plaintiffs seek restitution pursuant to the Consumer Protection Acts, and injunctive relief on behalf of the Class.

113. Plaintiffs seek attorney's fees and damages to the fullest extent permitted under the Consumer Protection Acts.

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

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

115. Defendant owns, licenses and/or maintains computerized data that includes

Plaintiffs' and Class Members' PII.

116. 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.

117. 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").

118. 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.

119. 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.

120. 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.

121. 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 . . . ."

122. 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.

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

124. 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.

125. 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).

126. 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 Plaintiff prays 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 enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity the type of PII compromised during the Data Breach;

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

E. Ordering Defendant to pay for not less than three years of credit card monitoring services for Plaintiffs and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class members and to post notice of the Breach in all affected stores;

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

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

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

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

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

DEMAND FOR JURY TRIAL

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

Respectfully submitted,

/s/ Jean Sutton Martin

Jean Sutton Martin
North Carolina State Bar No. 25703
Email: jean@jsmlawoffice.com
Law Office of Jean Sutton Martin PLLC
2018 Eastwood Road Suite 225
Wilmington, North Carolina 28403
Tel: (910) 292-6676
Fax: (888) 316-3489

Motion for Pro Hac Vice Admission to be filed for:

JONES WARD PLC
Jasper D. Ward
Marion E. Taylor Building
312 S. Fourth Street, 6th Floor
Louisville, Kentucky 40202
Tel: (502) 882-6000
Counsel for Plaintiff and Proposed Class

Morgan & Morgan Complex Litigation Group
John A. Yanchunis, Sr.
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
Counsel for Plaintiff and Proposed Class