FILED
2018 Jul-10 AM 10:05
U.S. DISTRICT COURT
N.D. OF ALABAMA

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA

ANNA CARROLL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MACY'S INC., MACY'S RETAIL HOLDINGS, INC., and MACY'S SYSTEMS AND TECHNOLOGY, INC.

Defendants

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff ANNA CARROLL brings this class action against Defendants MACY'S INC., MACY'S RETAIL HOLDINGS, INC., and MACY'S SYSTEMS AND TECHNOLOGY, INC. on behalf of herself and others similarly situated to obtain damages, restitution and injunctive relief for the Class, as defined, below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

PARTIES

1. Plaintiff is an individual who resides in this Judicial District. Plaintiff has an online account with Macys.com, accessible through a username and password. Macys.com stored Plaintiff's personal information, including her s name, address, phone number, email address, birthday and credit card number with expiration date. Plaintiff has made multiple online purchases from Macys.com using her Macys.com account, including between April 26 and June 6. On, July

7, 2018, DefendantS notified Plaintiff that she was the victim of data breach and that a third party had likely obtained the personal information contained in Plaintiff's Macy's.com account.

2. Defendant Macy's, Inc., Macy's Retail Holdings, and Macy's System and Technology, Inc. are headquartered in Cincinnati, Ohio. Defendants operates Macy's and Bloomingdale's department stores and websites. Defendants do business in this District, both through Macys.com and Bloomingdales.com ("Defendant's Websites") and through retail stores they operate within this District. Defendants are one of the largest clothes retailers and department store chains in the world, with annual revenues in excess of $20 billion.

JURISDICTION AND VENUE

3. 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 Defendants, and the amount in controversy exceeds $5 million.

4. This Court has personal jurisdiction over Defendants because Defendants are authorized to and conduct substantial business in Alabama, generally, and this District, specifically. Defendants own and operate retail locations within this District and throughout Alabama.

5. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1), because a substantial part of the events and omissions giving rise to this action occurred in this District as Defendants operate retail locations within this District, Plaintiff resides here, and Plaintiff made purchases from Macys.com within this District.

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

6. Millions of Americans regularly shop at Defendants' online and brick-and-mortar stores. When individuals transact business with Defendants via Defendants' Websites, or simply

visit those websites, Defendants collect a wide variety of Personally Identifiable Information (PII) about them.

7. Defendants disclose the information it collects about individuals who shop online– or simply browse their websites, even without making a purchase – on their websites:

> We collect information from a variety of sources, including: information provided by you, transaction information, technology-enabled services, and information we collect about you from third party sources. The following are select examples of the types of information we may collect and share:
>
> Information you provide: (FUL, ADV, OPS, SEC)
> We collect various information when you create a profile, place an order, create a registry or take advantage of other programs online or in store. Information we may collect includes: **Name, Address (billing and shipping), Zip code, email address, Telephone number(s), Cellular phone number(s), Credit card number(s), Birth date, and Security question answers.** (To express your preferences related to information you provide, go to the Manage Your Preferences section below).
>
> Technology-Enabled Collection Services: (FUL, ADV, OPS, SEC)
> We collect data when you visit our websites, use our mobile applications, shop in our stores, or interact with our wireless services and other technologies. This information is either automatically collected or is customer initiated. (For more details, see Our Use of Information Technologies section below).
>
> Transaction Information: (FUL, ADV, OPS, SEC)
> Transaction Information includes items purchased and date and time of your transaction, for in-store or online purchases.
> When you make a purchase or create a gift registry, we may share information about you and your transaction with other companies necessary to process your transaction or offer you products or services that may be of interest.
>
> MyClient (Clienteling/Client Book) (FUL, ADV, OPS, SEC)
> While in our stores, a Macy's sales associate(s) may ask your permission to enter your information into their client book. This is so that the associate can communicate with you on a one-to-one basis about Macy's products, services, and promotions that may be of interest to you or fulfill orders at your requests. Information sales associates collect includes: Name, Telephone number(s), Email, Credit card number (so transactions may be made on the client's behalf and at your request) and Address (billing and shipping). Information stored in our client book may be accessed and used by other Macy's personnel. (To express your preferences related to MyClient, go to the Manage Your Preferences section below.)

> Affiliate & Subsidiary Sharing: (FUL, ADV, OPS, SEC)
> We may share your information within Macy's, Inc., its affiliates, and subsidiaries (including Bloomingdale's and Bluemercury). This Notice does not cover the privacy practices of Bloomingdale's or Bluemercury.
>
> Third Parties: (FUL, ADV, OPS, SEC)
> We may receive your updated shipping information from a third party carrier.
> We may collect or use information made available to us through third party platforms, online databases and directories, or other means. We specify that data sourced from a third party must be legitimately and legally obtained. Some or all of this information may be governed by the privacy statements of the third party.
> We may share information with third parties who provide services to us or who work with us to offer products or services online or in our stores. Macy's also may share information with third parties so that they may directly offer their products or services to you if we think they may be of interest to you.
> We participate in consortiums with partners to share information or match (look alike or similar) customer data. When shared, this information is de-identified or anonymized.

https://www.customerservice-macys.com/app/answers/detail/a_id/40 (last visited July 9, 2018)(emphasis added).

8. Macys.com further boasts that:

> As a company, Macy's takes the security of your account information very seriously. Therefore, we take measures to protect the security of our customer's account information.

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

VALUE OF PII TO HACKERS AND LACK OF SEGREGATION OF CARD HOLDER DATA

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

11. Legitimate organizations and the criminal underground alike recognize the

value in PII. Otherwise, they wouldn't pay for it or aggressively seek it.

12. 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 privacy of Plaintiff's and Class Members' PII was lackadaisical, cavalier, reckless, and negligent.

13. 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.

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

15. One PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code. *Id*. at 7.

16. "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 personally identifiable information (PII) and corporate data." *See* Verizon 2014 PCI Compliance Report, available at http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf (hereafter "2014 Verizon Report"), at 54.

17. As noted in the 2014 Verizon Report, in "one of 2013's largest breaches . . .

not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users." *Id.* Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id.* Illicitly obtained PII and PCI, sometimes aggregated from different data breaches, 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 March 4, 2014).

18. Moreover, PII of individuals with something in common is extremely valuable to criminals because it can help them perpetrate targeted spear phishing attacks. Spear phishers target select groups with something in common, i.e., they shop at Macy's, so that they can send members of the group an email that looks just like an email from Macy's. But once recipients click on a link, they can be tricked into downloading malware on their own computers or deceived into giving up additional confidential information such as new passwords, financial information, personal data and much more.

THE DATA BREACH AFFECTING MACY'S

19. Defendants' security tools detected signs of a cyberattack by a third party on June 11, 2018. That third party had access to customer accounts, including Plaintiff's customer account, from April 26 to June 12, 2018.

20. Nevertheless, Defendants waited almost a month before notifying customers of the attack.

21. Sometime during the first week in July, Defendants mailed to affected customers, including Plaintiff, a letter notifying customers of "suspicious login activities" by

a third party and informing customers that the third party was able to access customer's name, address, phone number, email address, birthday and credit card or debit card number with expiration dates.

22. On July 9, 2018, Macy's spokesperson Blair Rosenberg confirmed the incident to Email Insider, providing a written statement confirming the breach:

> We are aware of a data security incident involving a small number of our customers at macys.com and bloomingdales.com. We have investigated the matter thoroughly, addressed the cause and, as a precaution, have implemented additional security measures. Macy's, Inc. will provide consumer protection services at no cost to those customers. We have contacted potentially impacted customers with more information about these services.

23. While Defendants indicated that social security numbers or the security numbers that appear on the back of cards were not compromised, they have not disclosed whether the wide range of other PII that it collects were disclosed in the breach.

24. By Defendants' own admission, hackers may had access to Defendants' information systems for over two weeks.

25. 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. On information and belief, while hackers scoured Defendants' networks to find a way into the POS, they had access to and collected PII stored on Defendants' networks.

CONSEQUENCES OF DEFENDANTS' CONDUCT

26. 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.

27. The ramifications of Defendant's failure to keep class members' data secure

are severe.

28. The information Defendant lost, including Plaintiff's 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.a2gov.org/government/safetyservices/Police/Documents/FTC%20identity%20theft%20guide.pdf> (last visited Jan. 27, 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.* The FTC estimates that as many as 10 million Americans have their identities stolen each year. *Id.*

29. As the FTC recognizes, 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).

30. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud." *See* 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/276 >(last visited Mar. 4, 2014) ("2013 Identity Fraud Report"). 46% of consumers with a breached debit card became fraud victims within the same year. *Id.*

31. 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 the 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. Some of this activity may not come to light for years.

32. 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.

33. 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 "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Mar. 5, 2014). In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

34. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2008:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the

> victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The President's Identity Theft Task Force Report at p.21 (Oct. 21, 2008), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

35. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013. *See* 2013 Identity Fraud Report.

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

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

GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphasis added).

37. Given that 9,200 confirmed instances of fraud have already resulted from the Data Breach to date, Plaintiff and the Class she seeks to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

CLASS ACTION ALLEGATIONS

38. Plaintiff seeks relief in her 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 classes initially defined as follows:

THE NATIONWIDE CLASS:

All persons whose personal and/or financial information was disclosed in the data incursion affecting Macys in 2018. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

THE ALABAMA SUBCLASS:

All persons residing in Alabama whose personal and/or financial information was disclosed in the data incursion affecting Macys in 2018. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

39. 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 Plaintiff at this time, based on information and belief, it is in the millions.

40. 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 Defendants unlawfully used, maintained, lost or disclosed Class members' personal and/or financial information;

b. Whether Defendants unreasonably delayed in notifying affected customers of the data breach;

c. Whether Defendants 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 Defendants' conduct was negligent;

e. Whether Defendants' negligence caused harm to Plaintiff and the Class; and

f. Plaintiff and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

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

43. 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 the members of the Class 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.

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

45. Defendants have 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 the Nationwide Class)

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

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

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

49. Defendants had a duty to timely disclose that Plaintiff's Private Information within their possession might have been compromised.

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

51. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff by failing to exercise reasonable care in protecting and safeguarding Plaintiff's Private Information within Defendants' possession.

52. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's Private Information.

53. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and class members the fact that their Private Information within their possession might have been compromised.

54. Defendants' negligent and wrongful breach of their duties owed to Plaintiff

and the Class proximately caused Plaintiff's and Class members' Private Information to be compromised.

55. Defendants' breach caused Plaintiff to suffer fraud, temporary loss of use of their credit or debit cards, and loss of time and money monitoring her finances for future fraud.

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

SECOND COUNT
Violation of Alabama's Deceptive Trade Practices Act
(On the Alabama Subclass)

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

58. As fully alleged above, Defendants engaged in unfair and deceptive acts and practices in violation of Alabama Code §8-9-1 et seq.

59. Reasonable consumers would be misled by Defendants' misrepresentations and/or omissions concerning the security of their personal information, because they assume retail companies that take credit and/or debit card information and collect PII from online shoppers will properly safeguard that Private Information in a manner consistent with industry standards and practices.

60. Defendants' did not inform customers that it failed to properly safeguard their Private Information, thus misleading Plaintiff and Class members in violation of §8-9-1 et seq. Such misrepresentation was material because Plaintiff and Class members entrusted Defendants with their Private Information when shopping online.

61. Had Plaintiff and Class members known of Defendants' failure to maintain adequate security measures to protect their Private Information, Plaintiff and Class members

would not have made online purchases at Defendants' Websites or otherwise entrusted their Private Information to Defendants.

62. As a direct and proximate result of Defendants' violations, Plaintiff and the Class suffered injury in fact and loss, including fraud, temporary loss of use of their credit or debit cards, and loss of time and money monitoring their finances for future fraud.

63. Plaintiff seeks restitution and injunctive relief on behalf of the Class.

64. Plaintiff seeks attorney's fees.

JURY DEMAND

Plaintiff demands a trial by jury of all claims in this Complaint so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendants, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;

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

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

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

E. For an award of punitive damages;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

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

Dated: July 9, 2018

/s/ Oscar M. Price, IV

Oscar M. Price, IV
PRICE ARMSTRONG, LLC
2226 1st Ave. S, Ste. 105
Birmingham, AL 35233
Phone: 205.208.9588
Fax: 205.208.9598
oscar@pricearmstrong.com

Counsel for Plaintiff and the Proposed Class

DEFENDANTS MAY BE SERVED AT THIS ADDRESS:

Corporate Creations Network, Inc.
6 Office Park Circle #100
Mountain Brook, AL 35223