UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE HUDSON'S BAY COMPANY DATA SECURITY INCIDENT CONSUMER LITIGATION	**Civil Action No. 18-cv-8472 (PKC)**
	CONSOLIDATED AMENDED CLASS ACTION COMPLAINT
	JURY TRIAL DEMANDED

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Bernadette Beekman, Debbie Carthan, John Cona, Wendy Haggarty, Julia A. Harris, Cassondra Joseph, Margo Kyler Knight, Jane Lefkowitz, Leslie Levitt-Raschella, Kelly McGurn, Dennis Meduri, Georgina Meduri, Greta Moss, Larry Payne, Alexandria Rudolph, Jeanne Sacklow, Hope Tafet, Erika Targum, Latusha Vains and Mark Wade ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts respectively pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Consolidated Amended Class Action Complaint against defendants Hudson's Bay Company ("HBC"); Saks Incorporated, Saks Fifth Avenue LLC, Saks & Company LLC (collectively, "Saks"); and Lord & Taylor LLC ("Lord & Taylor") (all Defendants are collectively referred to as "Defendants").

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendants for their failure to exercise reasonable care in securing and safeguarding their customers' personal financial data—including

credit and debit card records including cardholder name, card number, expiration date, and internal verification code ("Private Information" or "PI").

2. On March 28, 2018, a criminal syndicate known as "JokerStash" announced the release for sale on the dark web of stolen credit and debit card records from a cache of over five million stolen records. The cybersecurity firm Gemini Advisory determined that the cards were misappropriated in a breach involving Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor retail stores ("Security Breach") owned and operated by Defendants during the period between no later than May 2017 and late-March 2018.

3. On April 1, 2018, Defendants announced that they "became aware of a data security issue involving customer payment card data."

4. On April 27, 2018, Defendants announced that the Security Breach lasted nine months going back to around July 1, 2017, and that the hackers had placed malware on Saks' and Lord & Taylor's retail systems in order to collect customer PI when Plaintiffs and Class members used their credit and debit cards at Defendants' stores.

5. On information and belief, Plaintiffs' and Class members' Private Information was stolen by hackers in order to be sold on the dark web.

6. Defendants' security failures enabled the hackers to steal Plaintiffs' and Class members' Private Information. The failures put Plaintiffs' and Class members' financial information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Security Breach, including, as appropriate, finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft

protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach. The hackers will continue to sell the Private Information—and cyber criminals will continue to buy and use it—in order to exploit and injure Plaintiffs and Class members across the United States.

7. The Security Breach was caused and enabled by Defendants' violation of their obligations to abide by best practices and industry standards concerning the security of payment systems. Defendants failed to comply with security standards and allowed their customers' Private Information to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

8. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, assert claims for violations of state consumer statutes, negligence, breach of confidence, breach of implied contract, and unjust enrichment/quasi-contract, and seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

9. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. The Court has personal jurisdiction over Defendants because their principal place of business is located, and they conduct substantial business, in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants maintain their principal place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2).

III. PARTIES

Plaintiffs

12. Plaintiff Bernadette Beekman is a resident of New York. In May of 2017, Plaintiff Beekman used a credit card to pay for purchases at a Lord & Taylor retail store in New York City, and had her Private Information exposed as a result of Lord & Taylor's inadequate security. Plaintiff Beekman has paid for LifeLock theft monitoring services every year since 2016. She decides whether to renew March 19 of each year. She pays annually $219.89 for LifeLock. In March 2019, following the Security Breach, she decided to renew her LifeLock coverage as she was concerned about her information having been exposed. She also pays a bookkeeper $50 per month which includes monitoring for suspicious or fraudulent activity in her financial and credit accounts. She has continued paying the bookkeeper after the Security Breach as she is concerned about her information having been exposed. Immediately after and as a result of the Security Breach, she spent time inspecting her credit card statements for fraudulent activity and researching the breach on the Internet (approximately two hours). She has suffered from the deprivation of the value of her Private Information. Plaintiff Beekman would not have shopped at Lord & Taylor had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

13. Plaintiff Debbie Carthan is a resident of New Jersey and made several purchases from affected Saks and Lord & Taylor stores during the period of compromise using her debit card and/or credit card, and had her Private Information exposed as a result of Saks' and Lord & Taylor's

inadequate security. Plaintiff Carthan subsequently experienced credit fraud, which required her to freeze or cancel one or more of her individual accounts and/or monitor her accounts. In particular, she was forced to call TD bank and change her PIN on her debit card multiple times because of fraudulent attempts to use her card to purchase merchandise such as shoes, coffee at Dunkin Donuts, food at Popeye's Chicken, coffee at Starbucks, and gasoline at a gas station in Long Island, NY. In addition. Plaintiff Carthan has continued to receive fraudulent emails seeking personal information since the Security Breach. Due to the fraudulent attempts or activity on her accounts and fraudulent email attempts to obtain her Private Information, Plaintiff Carthan has spent numerous hours researching issues regarding the data breach, traveling to Saks and discussing with customer service the data breach and fraudulent activity, traveling to her banks and discussing with representatives the data breach and fraudulent activity, contacting her banks and credit card companies regarding the data breach and fraudulent activity, and monitoring her accounts to safeguard against fraud and theft and addressing issues from the Security Breach. She has suffered from the deprivation of the value of her Private Information. Plaintiff Carthan would not have shopped at Saks or Lord & Taylor had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

14. Plaintiff John Cona is a resident of New York. He made several purchases at affected Saks and Lord & Taylor stores in New York during the relevant time period of the compromise and purchased merchandise using a debit or credit card and had his Private Information exposed as a result of Saks' and Lord & Taylor's inadequate security. Plaintiff Cona subsequently experienced credit fraud, which required him to freeze or cancel one or more of his individual accounts. Due to the fraudulent attempts or activity on his accounts, Plaintiff Cona has

spent numerous hours researching issues regarding the data breach, contacting his banks and credit card companies to freeze and cancel accounts and monitoring his accounts to safeguard against fraud and theft and addressing issues from the Security Breach. Plaintiff Cona continues to spend numerous hours monitoring his accounts to safeguard against fraud and theft and addressing issues from the Security Breach. He has suffered from the deprivation of the value of his Private Information. Plaintiff Cona would not have shopped at Saks or Lord & Taylor had Defendants told him that they failed to maintain adequate computer systems and data security practices to safeguard his Private Information from theft.

15. Plaintiff Wendy Haggarty is a resident of Pennsylvania. She shopped at an affected Saks Fifth Avenue store several times during the relevant time period and each time paid with a debit card and had her Private Information exposed as a result of Saks' inadequate security. Plaintiff Haggarty subsequently experienced fraudulent activity on her account and received over eleven emails from orders@saks.com regarding orders being made on her account, which required her to spend numerous hours investigating these orders by contacting representatives of Saks about these fraudulent orders. She has also suffered from the deprivation of the value of her Private Information. Plaintiff Haggarty would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

16. Plaintiff Julia A. Harris is a resident of Connecticut and shopped at Lord & Taylor in Connecticut and New York and had her Private Information exposed as a result of Lord & Taylor's inadequate security. Plaintiff Harris learned of the data breach at Lord & Taylor in or about early April 2018. Upon learning of this breach, Harris undertook to investigate the circumstances of the breach by conducting a personal investigation on the Internet, and therefore

expended time and energy investigating the breach. Based upon that investigation, she subsequently determined to contact an attorney and discussed her potential exposure with an attorney, and again spent time and energy in speaking with counsel. Harris continues to have the credit card that was used at Lord & Taylor and is the subject of the data breach and continues to expend time and energy to monitor her credit card account for suspicious or unauthorized activity. She has suffered from the deprivation of the value of her Private Information. Plaintiff Harris would not have shopped at Lord & Taylor had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

17. Plaintiff Cassondra Joseph is a resident of New York. She shopped at several different affected Saks Fifth Avenue stores in New York and Lord & Taylor's flagship store in New York (prior to its recent closing) during the relevant time period and purchased merchandise using two different credit cards and had her Private Information exposed as a result of Saks' and Lord & Taylor's inadequate security. In particular, the first card, issued by Chase Bank, has already been used by criminals to make fraudulent charges. Plaintiff Joseph has spent numerous hours monitoring her accounts to safeguard against fraud and theft and addressing issues from the Security Breach – including challenging the Bank's original denial of coverage of the fraud (approximately five hours). She still has this card. Her second card has not yet been the subject of any fraudulent charges to her knowledge and she must now expend additional time and effort to diligently review her statements to determine whether this card too will be subject to fraud. She has also suffered from the deprivation of the value of her Private Information. Plaintiff Joseph would not have shopped at Saks or Lord & Taylor had Defendants told her that they failed to

maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

18. Plaintiff Margo Kyler Knight is a resident of Arizona and made several purchases from an affected Saks OFF 5TH store during the relevant time-period using her credit card and had her Private Information exposed as a result of Saks' inadequate security. Plaintiff Knight subsequently experienced fraud, which required her to freeze and/or cancel one or more of her individual accounts. Due to the fraudulent attempts or activity on her accounts, Plaintiff Knight also has spent numerous hours monitoring her accounts to safeguard against fraud and theft and addressing issues from the Security Breach (approximately 35 hours). She has also suffered from the deprivation of the value of her Private Information. Plaintiff Knight would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

19. Plaintiff Jane Lefkowitz is a resident of Florida. She shopped at an affected Saks Fifth Avenue store on January 8, 2018 and used her Visa credit card for this purchase and had her Private Information exposed as a result of Saks' inadequate security. As a result of the Security Breach, she spent time inspecting her credit card statements as well as her bank account statements for fraudulent activity on a weekly basis which took between five and ten minutes each time. In addition, on or around September 7, 2018, Plaintiff Lefkowitz received a new Visa credit card, to replace the card she had used at Saks, from Visa due to a data compromise. She has also suffered from the deprivation of the value of her Private Information. Plaintiff Lefkowitz would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

20. Plaintiff Leslie Levitt-Raschella is a resident of New York. On November 13, 2017 she shopped at an affected Saks Off 5TH store and an affected Lord & Taylor store in New York and purchased merchandise with a debit card and had her Private Information exposed as a result of Saks' and Lord & Taylor's inadequate security. As a result of the Security Breach, she spent time inspecting her credit card statements for fraudulent activity and monitoring other accounts such as bank accounts. Plaintiff Levitt-Raschella subsequently experienced credit fraud and identity theft, which required her to freeze and/or cancel many of her individual accounts and monitor her accounts. Her identity theft included the breach of her name, address, social security number and date of birth. Numerous accounts were fraudulently opened in her name without her authorization including a TD Bank account and AT&T account as well as credit card accounts which include Kohl's and Williams Sonoma. The fraudulent TD Bank account was opened initially online with Plaintiff's social security number, name and date of birth and then an individual physically went into a TD Bank to make a deposit in that account. This account was linked to the fraudulent AT&T account that was opened in Plaintiff's name. Plaintiff subsequently received a TD Bank statement that was in her name but was not an account she opened. Her Amazon account was fraudulently compromised, and her Instagram account was taken over by another individual who locked her out of the account. Due to the fraudulent attempts or activity on her accounts, Plaintiff Levitt-Raschella has spent significant hours monitoring her accounts to safeguard against fraud and theft and addressing issues from the Security Breach which included the filing of a police report with the Suffolk County Police Department, Identity Theft Section. In addition, Levitt-Raschella spent significant hours contacting each of the credit bureau agencies in order to notify them of her identity theft and requested that her credit be frozen. Levitt-Raschella had numerous fraudulent charges to her credit and debit cards. She has also suffered from the

deprivation of the value of her Private Information. Plaintiff Levitt-Raschella would not have shopped at Saks or Lord & Taylor had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

21. Plaintiff Kelly McGurn is resident of Georgia. She shopped at an affected Saks Fifth Avenue store and an affected Lord & Taylor store in Philadelphia, Pennsylvania during the relevant period of compromise and each time paid with a debit card and had her Private Information exposed as a result of Saks' and Lord & Taylor's inadequate security. Plaintiff McGurn subsequently experienced credit fraud, which required her to freeze or cancel one or more of her individual accounts and/or monitor her accounts. As a result of the Security Breach, she also purchased identity theft and credit monitoring for a period of six months for $174 ($29 per month). Due to the fraudulent attempts or activity on her accounts, Plaintiff McGurn has spent numerous hours researching issues regarding the data breach, contacting her banks and credit card companies about the data breach and fraudulent activity, monitoring her accounts to safeguard against fraud and theft, and addressing issues from the Security Breach. Plaintiff McGurn continues to spend numerous hours monitoring her accounts to safeguard against fraud and theft and addressing issues from the Security Breach. She has also suffered from the deprivation of the value of her Private Information. Plaintiff McGurn would not have shopped at Saks or Lord & Taylor had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

22. Plaintiff Dennis Meduri is a resident of New York. He shopped at an affected Lord & Taylor store in New York during the period of compromise and purchased merchandise using his American Express credit card and had his Private Information exposed as a result of Lord & Taylor's inadequate security. He has suffered from the deprivation of the value of his Private

Information. Plaintiff Dennis Meduri would not have shopped at Lord & Taylor had Defendants told him that they failed to maintain adequate computer systems and data security practices to safeguard his Private Information from theft.

23. Plaintiff Georgina Meduri is a resident of New York. She shopped at an affected Lord & Taylor store in New York during the period of compromise and purchased merchandise using an American Express card and a bank debit card and had her Private Information exposed as a result of Lord & Taylor's inadequate security. She has suffered from the deprivation of the value of her Private Information. Plaintiff Georgina Meduri would not have shopped at Lord & Taylor had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

24. Plaintiff Greta Moss is a resident of Illinois. She shopped at affected Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor stores in Illinois during the period of compromise and with both debit and credit cards issued by Chase and had her Private Information exposed as a result of Saks' and Lord & Taylor's inadequate security. Plaintiff Moss subsequently experienced fraud on her credit card, which required her to cancel her debit card, credit card, file a police report with the Homewood Illinois Police Department on December 7, 2017 with respect to the fraudulent activity on her credit card and file a report with the FTC on December 8, 2017 reporting the identity theft and fraudulent charges on her account. As a result of the Security Breach and fraudulent activity, she spent numerous hours researching issues regarding the data breach, inspecting her credit card and bank statements, canceling her accounts, filing a police report, filing a report with the FTC, as well as monitoring her accounts for fraudulent activity. Plaintiff Moss continues to spend numerous hours monitoring her accounts to safeguard against fraud and theft and addressing issues from the Security Breach. She has also suffered from the deprivation of the value of her

Private Information. Plaintiff Moss would not have shopped at Saks or Lord & Taylor had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

25. Plaintiff Larry Payne is a resident of Kentucky. He shopped at an affected Lord & Taylor store during the period of compromise and paid with credit cards issued by Capital One and Lord & Taylor and had his Private Information exposed as a result of Lord & Taylor's inadequate security. Plaintiff Payne subsequently experienced credit fraud, which required him to spend numerous hours to freeze and/or cancel one or more of his individual accounts and/or monitor his accounts. In this regard, Plaintiff Payne noticed a number of unauthorized purchases on his Capital One billing statement from Lord & Taylor stores in Michigan, New York and other locations which he never purchased from or visited. As a result, he called Lord & Taylor customer service and spoke with a representative who pulled up his account and informed him that these were online credit card purchases. Plaintiff Payne continued his investigation and spent additional time looking into the charges and confirmed that none of the products were purchased by him or his wife. As a result, he notified Capital One about the fraudulent charges, closed online access to the account and had a new credit card issued. In April 2018 as Plaintiff Payne's investigation continued, he spoke to a customer serve representative of Lord & Taylor regarding the fraudulent activity and the representative confirmed for him that his account was "hacked". In addition, Plaintiff Payne received over 1000 fraudulent emails seeking personal information and/or inquiries regarding credit and loan applications which required him to spend numerous hours to go through each email and unsubscribe to the credit and loan applications. Since the Security Breach, due to the fraudulent attempts or activity on his accounts, Plaintiff Payne has spent has spent numerous hours researching issues regarding the data breach, contacting his banks and credit card companies

regarding the data breach and fraudulent activity, reviewing thousands of emails regarding credit and loan applications, monitoring his accounts to safeguard against fraud and theft and addressing issues from the Security Breach. Plaintiff Payne continues to spend numerous hours monitoring his accounts to safeguard against fraud and theft and addressing issues from the Security Breach. He has also suffered from the deprivation of the value of his Private Information. Plaintiff Payne would not have shopped at Lord & Taylor had Defendants told him that they failed to maintain adequate computer systems and data security practices to safeguard his Private Information from theft.

26. Plaintiff Alexandria Rudolph is a resident of California. On November 23, 2017, Plaintiff Rudolph used her Visa debit card to purchase items at an affected Saks OFF 5TH store at 100 N. La Cienega Boulevard, Beverly Hills, California and had her Private Information exposed as a result of Saks' inadequate security. On May 18, 2018, Bank of America notified her of suspected fraudulent activity on the Visa debit card used during her November 2017 purchase at the Saks OFF 5TH retail location. As a result, Bank of America froze Plaintiff Rudolph's account associated with the payment card. Her payment card was compromised despite Plaintiff Rudolph having physical possession of the card at all times. Following the hold placed on her account, Plaintiff Rudolph spent approximately 20 minutes contacting Bank of America telephonically attempting to resolve the issue. Because Plaintiff Rudolph needed a new debit card immediately, she drove approximately 25 miles, which took her about one and a half hours, to visit a Bank of America branch in person to get a new card. In doing so, she expended cash in the form of gasoline to get to the bank. Specifically, Plaintiff Rudolph used approximately 1.20 gallons of gasoline driving to the bank, which cost her approximately $4.68. At the bank, she spent approximately 30 minutes discussing the account freeze with a banker and requesting and obtaining a new debit card.

Plaintiff Rudolph also spent approximately one hour looking through her account records after the account freeze. Further, since May 2018, she has expended approximately 30 minutes in total updating her payment cared information with various retailers. Finally, since May 2018, Plaintiff Rudolph has spent several hours reviewing monthly financial statements for any fraudulent or suspicious charges. Plaintiff would not have spent this time and money had it not been for the data breach. She has also suffered from the deprivation of the value of her Private Information. Plaintiff Rudolph would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

27. Plaintiff Jeanne Sacklow is a resident of New York. In March 2018, she used her credit card to make a purchase during the relevant period at an affected Saks Fifth Avenue store in New York City, and had her Private Information exposed as a result of Saks' inadequate security. As a result of the Security Breach, she called her credit card company and spent approximately 10 minutes on the telephonic discussing the security of her Personal Information. As a result of the Security Breach, she has spent five to ten minutes every month since the Security Breach carefully reviewing her credit card statements for fraudulent activity. She has also suffered from the deprivation of the value of her Private Information. Plaintiff Sacklow would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

28. Plaintiff Hope Tafet is a resident of New Jersey. She shopped at Saks OFF 5TH in New Jersey during the relevant time period and paid with a credit card issued by Saks and had her Private Information exposed as a result of Saks' inadequate security. Plaintiff Tafet's personal "profile" was included in the information held by Saks which included information about "other"

credit cards used for Saks purchases, including her American Express credit card information which she had used on other occasions. A month or so prior to the announcement of the Security Breach, Plaintiff Tafet received a fraudulent charge on her American Express card for the first time in 20 years. Although the fraudulent charge was reversed, it took 15 minutes to complete this process. As a result of the Security Breach, she spent time inspecting her credit card statements for fraudulent activity. She has also suffered from the deprivation of the value of her Private Information. Plaintiff Tafet would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

29. Plaintiff Erika Targum is a resident of New York. In May of 2017, she used a credit card to return a purchase to an affected Saks Fifth Avenue store in New York City, and had her Private Information exposed as a result of Saks' inadequate security. Plaintiff Targum has paid for LifeLock theft monitoring services every year since 2013. She decides whether to renew January 7 of each year. She pays annually $220.00 each for her and her husband and $52.79 each for her two children. In January 2019, following the Security Breach, she decided to renew her LifeLock coverage as she was concerned about her information having been exposed. Immediately after learning of the Security Breach, she spent time (approximately one hour) to put a temporary block on her credit card and set spending limits to prevent fraud and contacted LifeLock to ensure that there had been no fraudulent activity. As a result of the Security Breach, she has also spent time herself inspecting her credit card statements for fraudulent activity (approximately one hour per month) and continues to do so. Moreover, Plaintiff Targum spent time immediately after the announcement of the Security Breach (approximately 7.5 hours) during the first week of April 2018 researching and trying to understand how the Security Breach could

affect her privacy and credit, including through television, newspapers and the Internet, and also to check her credit score. She has also suffered from the deprivation of the value of her Private Information. Plaintiff Targum would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

30. Plaintiff Latusha Vains is a resident of California. During the Christmas shopping season, Plaintiff Vains made a purchase at a Saks store located in San Francisco, California. For this purchase, she used her American Express credit card and had her Private Information exposed as a result of Saks' inadequate security. In January 2018, Plaintiff Vains reviewed her American Express statement and identified fraudulent activity in the amount of $1,300. As a result of the Security Breach and the fraudulent activity, Plaintiff Vains had to spend time cancelling her American Express card, requesting a new one, and changing passwords associated with her American Express card and account. In addition, she has suffered from the deprivation of the value of her Private Information. Plaintiff Vains would not have shopped at Saks had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

31. Plaintiff Mark Wade is a resident of Texas and made several purchases from an affected Saks store and an affected Lord & Taylor store in Texas during the relevant time period using his credit card and had his Private Information exposed as a result of Saks' and Lord & Taylor's inadequate security. Plaintiff Wade subsequently experienced fraud when his debit card issued by Bank of America was used for fraudulent purchases and when money was withdrawn without his consent from accounts at TD Bank ($6,289.22), Bank of America ($2,294.26) and BBVA Compass. As a result of the Security Breach and fraudulent activity, he was required to

freeze or cancel one or more of his individual accounts including closing out his bank accounts at TD Bank, Bank of America and BBVA Compass. In addition, as a result of the Security Breach and fraudulent activity, he spent $260.00 and purchased identity theft and credit monitoring through Equifax. Due to the fraudulent attempts or activity on his accounts and fraudulent email attempts to obtain his Private Information, Plaintiff Wade has spent numerous hours researching issues regarding the data breach, contacting his banks and credit card companies regarding the data breach and fraudulent activity, monitoring his accounts to safeguard against fraud and theft, addressing issues from the Security Breach, and purchasing identify theft protection and credit monitoring services. In this regard, Plaintiff Wade spent numerous hours (days) driving over 2,246 miles from Las Vegas, Nevada to a TD Bank office in Jacksonville, Florida and back to Las Vegas to discuss the fraudulent withdrawal of funds and freezing and closing of his account with a TD Bank officer and incurred costs and expenses for gas, food and other incidental expenses. He also spent numerous hours speaking to representatives from Bank of America on the phone and representatives from BVAA Compass banks on the phone and in person which required him to drive to a branch in Las Vegas. Plaintiff Wade continues to spend numerous hours monitoring his accounts to safeguard against fraud and theft and addressing issues from the Security Breach. As a result of the Security Breach, he has suffered from the deprivation of the value of his Private Information. Plaintiff Wade would not have shopped at Saks or Lord & Taylor had Defendants told him that they failed to maintain adequate computer systems and data security practices to safeguard his Private Information from theft.

32. Plaintiffs and the other Class members are also at risk of imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being stolen by criminals in the Security Breach and sold on the black

market, including, but not limited to, the extent that Plaintiffs still have their credit or debit cards used at Defendants' stores.

33. Plaintiffs have a continuing interest in ensuring that their Private Information is protected and safeguarded from future breaches.

34. Plaintiffs also suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property that Plaintiffs entrusted to Defendants as a form of payment for merchandise and that was compromised in and as a result of the Security Breach, including, but not limited to, the extent that Plaintiffs still have their credit or debit cards used at Defendants' stores.

35. The injuries suffered by Plaintiffs and Class members as a direct result of the Security Breach include one or more of the following:

a. unauthorized use of their PI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PI;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal

with the actual and future consequences of the Security Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach;

g. the imminent and impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;

h. damages to and diminution in value of their PI entrusted to Defendants for the sole purpose of purchasing products and services from Defendants; and the loss of Plaintiffs' and Class members' privacy.

Defendants

36. Defendant HBC is a Canadian corporation that maintains its U.S. headquarters, and main base of operations, in New York, New York. HBC is the corporate parent of Defendant Saks Incorporated and Defendant Lord & Taylor LLC.

37. Defendant Saks Incorporated is a Tennessee corporation which operates a number of luxury department stores through one or more of its wholly owned subsidiaries under the Saks Fifth Avenue and Saks OFF 5TH banners, selling clothing, footwear, jewelry, beauty products, fragrances, electronics, bedding, and housewares. Saks Incorporated's principal place of business is in New York, New York.

38. Defendant Saks Fifth Avenue LLC is a Massachusetts limited liability company with its principal place of business in New York, New York. The sole member of Saks Fifth Avenue LLC is Defendant Saks & Company LLC, a Delaware limited liability company.

39. Defendant Saks & Company LLC is a Delaware limited liability company with its principal place of business in New York, New York. The sole member of Saks & Company LLC is Saks Incorporated, a Tennessee corporation.

40. Defendant Lord & Taylor LLC is a Delaware limited liability company which operates a number of luxury department stores selling clothing, footwear, jewelry, beauty products, fragrances, electronics, bedding, and housewares. Lord & Taylor LLC's principal place of business is in New York, New York. The sole member of Lord & Taylor LLC is Lord & Taylor Holdings LLC, a Delaware limited liability company with its principal place of business in New York, New York. The sole member of Lord & Taylor Holdings LLC is Lord & Taylor Acquisition Inc., a Delaware corporation with its principal place of business in New York, New York.

IV. FACTUAL BACKGROUND

The Security Breach

41. On March 28, 2018, a criminal syndicate known as "JokerStash" announced that it would be releasing for sale on the dark web stolen credit and debit card records from a cache of over five million stolen records.

42. "JokerStash" is a criminal syndicate trading in stolen debit and credit card data. Since its inception in 2014, JokerStash has attracted dozens of identity thief customers who have spent tens and hundreds of thousands of dollars on stolen credit card information.[1] As described by security researcher Brian Krebs, JokerStash offers its identity thief customers "loyalty

[1] Brian Krebs, *Carders Park Piles of Cash at Joker's Stash*, KrebsonSecurity (Mar. 16, 2016), https://krebsonsecurity.com/2016/03/carders-park-piles-of-cash-at-jokers-stash/. (last visited Aug. 9, 2019)

programs, frequent-buyer discounts, money-back guarantees and just plain old good customer service."[2]

43. The cybersecurity firm Gemini Advisory determined that the card records being advertised for sale by JokerStash were stolen from a breach involving Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor retail stores during the period between no later than May 2017 and late-March 2018.

44. The image below reflects a portion of JokerStash's advertisement for the stolen Private Information describing the card records as including "TR1" and "TR2" data, which includes cardholder names, card numbers, expiration dates, and internal verification codes.

45. On April 1, 2018, nearly a year after hackers first began collecting the Private Information of Plaintiffs and other Class members, and only after Gemini forced its hand by publicly implicating it, Defendant HBC announced that it "became aware of a data security issue

[2] *Id.*

involving customer payment card data[.]"[3] HBC's announcement misleadingly states, "We want to assure our customers that they will not be liable for fraudulent charges that may result from this matter"—without announcing any intention that Defendants will themselves compensate their customers for their damages.[4]

46. While HBC indicated in the April 1, 2018 Press Release that it will offer those impacted free identity protection services, including credit and web monitoring, credit monitoring is not a panacea because it is reactionary—it does nothing to prevent fraud in the first instance. As reported on *Krebs*, a leading security website:[5]

> [Credit monitoring services] are basically PR vehicles for most of the breached companies who offer credit report monitoring to potentially compromised consumers… it does absolutely nothing to compensate for the fact that a criminal stole credit card mag stripe account… [Credit monitoring services] only give consumers limited help with a very small percentage of the crimes that can be inflicted on them… [a]nd consumers can get most of that limited help for free via the government website or free monitoring from a breached entity where their data inevitably was compromised.

Reasonable consumers, however, still may resort to obtaining credit monitoring protection because it is almost always advised by the breached merchant, as was the case with Saks and Lord & Taylor, it is offered by reputable companies, and purports to provide security and monitoring service of value to consumers.

47. On April 27, 2018, Defendant HBC reported, among other things, that it believed that "[a]round July 1, 2017, malware began running on certain point of sale systems at potentially

---

[3] Stuart Lauchlan, *For Hudson's Bay's New CEO, Another Headache – a Data Breach With A Claimed 5 Million Cards At Risk*, Diginomica, (Apr. 2, 2018), https://diginomica.com/for-hudsons-bays-new-ceo-another-headache-a-data-breach-affecting-5-million-cards. (last visited Aug. 9, 2019)

[4] *Id.*

[5] Brian Krebs, *Are Credit Monitoring Services Worth It*, KrebsonSecurity, (Mar. 19, 2014), https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/comment-page-1/. (last visited Aug. 9, 2019)

all Lord & Taylor, Saks Fifth Avenue and Saks OFF 5TH locations in North America" and further that such "malware was designed to collect customers' payment card information, including cardholder name, payment card number and expiration date." This announcement also stated that HBC contained the data breach issue by March 31, 2018.[6]

48. Following the breach, Mark Cline, Vice President of the data-security firm Netsurion, stated that "[t]his incident shows once again merchants still need to protect themselves against POS system infiltration attacks targeting cardholder data. A multi-layer security strategy is necessary."[7] If such measures were in place, "[i]f nothing else, dwell time of such an attack would be reduced to hours or days."[8]

Defendants' Acts, Omissions, and Individuals Responsible for Data Security Were Concentrated in New York

49. Defendants' acts and omissions leading up to the Security Breach, including the individuals responsible for maintaining data security and consumers' PI, were heavily concentrated in New York.

50. As Saks previously stated, "the people and teams that direct [HBC]'s data security infrastructures are based largely in New York," and "the events involved in this action clearly have their center of gravity in and around New York[.]" [9] Indeed, the "Hudson's Bay Company employees who know about and implement Hudson's Bay Company's information security

[6] A copy of the release entitled "HBC Provides Update on Previously-Announced Data Security Issue at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor Locations in North America", is available at https://www.sedar.com/GetFile.do?lang=EN&docClass=8&issuerNo=00033738&issuerType=03&projectNo=02761956&docId=4304164 (last visited Aug. 8, 2019).
[7] Teri Robinson, *Saks, Lord & Taylor breached, 5 million payment cards likely compromised*, SC Media (Apr. 1, 2018), *available at* https://www.scmagazine.com/saks-lord-taylor-breached-5-million-payment-cards-likely-compromised/article/755180/.(last visited Aug. 9, 2019)
[8] *Id.*
[9] Mem. of Points and Authorities in Supp. of Def. Mot. to Dismiss at 2-3, 9, *Rudolph v. Saks & Company LLC*, No. 1:18-cv-08472-PKC (C.D. Cal. Aug. 20, 2018), ECF No. 18-1.

practices," who "discovered, analyzed, and managed the [Security Breach]," and were "involved in Defendant's record-keeping and data retention relating to customer purchase histories" all are located in New York."[10]

51. Further, the "public statements about the incident", including the notices sent to Plaintiffs and Class members regarding the Security Breach, "were all developed and issued from New York" by people "based in New York."[11]

Defendants' Prior Security Breach and Own Admissions Demonstrate Awareness of Insufficient Data Security Standards

52. Defendants' failure to adequately protect Private Information was not isolated to the 2017-2018 breach. Previously, in March 2017, HBC inadvertently "exposed the personal information of tens of thousands of [Saks Fifth Avenue] customers through the company's websites"[12] to the public.[13] Therefore, Defendants were fully aware of their lax data-security standards months before JokerStash successfully breached Defendants' security systems. According to Robert Graham, cybersecurity expert and owner of Errata Security, "[t]his is bad as security gets … [e]veryone is vulnerable."[14] An HBC spokesperson responded that "[w]e take this matter seriously …[t]he security of our customers is of utmost priority."[15] Once Defendants knew that their customers' personal information was exposed to the public, Defendants became aware, or should have become aware, that their data-security practices were insufficient.

---

[10] *Id.* at 16.
[11] *Id.* at 3-4.
[12] Emma Orr, *Hudson's Bay exposes Saks customer info online*, The Globe and Mail (Mar. 20, 2017), *available at* https://www.theglobeandmail.com/report-on-business/hudsons-bay-exposes-saks-customer-info-online/article34346027/. (last visited Aug. 9, 2019)
[13] Leticia Miranda, *Saks Fifth Avenue Exposed Personal Info on Tens of Thousands of Customers*, Buzzfeed (Mar. 19, 2017), available at https://www.buzzfeed.com/leticiamiranda/saks-fifth-avenue-exposed-personal-info?utm_term=.navJN3B8E#.rrRG2Bpqr. (last visited Aug. 9, 2019)
[14] *Id.*
[15] *Id.*

53. In April 2017, one month following the March 2017 breach of its customer's personal data, HBC issued its Annual Information Form, admitting that "[a] potential privacy breach could have a material adverse effect on our business and results of operations."[16] HBC further recognized that "[o]ur security measures may be undermined due to the actions of outside parties, employee error, malfeasance, and, as a result, an unauthorized party may obtain access to our data systems and misappropriate business and personal information."[17] HBC was admittedly aware of the severe risks involved in a failure to maintain proper data security standards. Following the March 2017 breach of the personal information of tens of thousands of their customers, immediate action should have been taken to increase the pre-existing data security measures in place for Defendants' stores. Defendants failed to do so.

Defendants Had Notice of Security Breaches Involving Malware on POS Systems

54. Defendants use a payment system to electronically process their customers' credit and debit card payments. In the years preceding HBC's announcement of the Security Breach, several retail outlets made announcements alerting the public of security breaches at their stores, including Barnes & Noble, Home Depot, Neiman Marcus, Michaels, Target, and TJ Maxx. Defendants knew or should have known that their customers' card data was squarely within the crosshairs of hackers. Despite this, Defendants failed to take adequate steps to secure the payment system used in their stores and allowed their customers' card data and PI to be hacked and stolen.

55. A point of sale system (POS) is an on-site device that manages payment card transactions from customer purchases. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and

[16] Hudson's Bay Company, Annual Information Form, at 61 (Apr. 28, 2017).
[17] *Id.*

networks before reaching the retailer's payment processor."[18] Before transmitting customer data over the merchant's network, POS systems typically, and very briefly, store the data in plain text within the system's memory.[19] Likewise, when an EMV chip-based payment card is used at a POS terminal, "'[i]nstead of going to a register and swiping your card, you are going to do what is called 'card dipping' instead, which means inserting your card into a terminal slot and waiting for it to process[.]'"[20]

56. As with a magnetic stripe card, "'[w]hen an EMV card is dipped, data flows between the card chip and the issuing financial institution to verify the card's legitimacy and create the unique transaction data."[21] According a leading payment processor: "[c]urrently, in the majority of both EMV and non-EMV transactions, payment card information is sent from the point-of-capture to the acquirer/processor 'in the clear,' i.e., in an unencrypted form."[22] Any time that payment card data is "in the clear" – that is, in plain text format that is readable by a person or computer – it is extremely vulnerable to theft. It is this unencrypted payment card data on the POS system that hackers seek to access.

57. It is well known that payment card data has significant value and often is targeted by hackers, who easily can sell it because of the "proliferation of open and anonymous cybercrime

---

[18] *SECURITY RESPONSE: A Special Report on Attacks on point-of-sales systems* at 6, SYMANTEC CORP. (Nov. 20, 2014), https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf. (last visited Aug. 9, 2019)
[19] *Id.* at 5.
[20] Sienna Kossman, *8 FAQs about EMV credit cards*, CREDITCARDS.COM (Aug. 29, 2017), https://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php (last visited Aug. 9, 2019).
[21] *Id.*
[22] *EMV and Encryption + Tokenization: A Layered Approach to Security* at 5, FIRST DATA CORP. (2012), https://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF. (last visited Aug. 9, 2019)

forums on the Dark Web that serve as a bustling marketplace for such commerce."[23] "As long as compromised credit card data continues to be a valuable commodity on the black market, any company collecting or processing valid credit card information will continue to be a high value target[.]'"[24] Hackers who access payment card data can physically replicate the card or use it online.

58. A number of data breaches have occurred at large retailers all over the country in recent years, including Target, Home Depot, Eddie Bauer, Sally Beauty, Harbor Freight Tools, and Kmart, among many others. Each of these massive data breaches involved malware placed on the merchant's POS system. For example, in 2013, hackers infiltrated Target's POS system, stealing information from an estimated 40 million payment cards in the United States.[25] In 2014, over 7,500 self-checkout POS terminals at Home Depot locations throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[26] In 2016, on-site POS systems at more than 1,000 Wendy's restaurants were infiltrated with malware, resulting in the theft of payment card data for nearly six months.[27]

59. Indeed, the susceptibility of POS systems to malware is well-known throughout the retail industry as a wave of data breaches causing the theft of retail payment card information has

---

[23] Brian Krebs, *The Value of a Hacked Company*, KrebsonSecurity (July, 16, 2016), https://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/. (last visited Aug. 9, 2019)
[24] Dan Rayward, *Chipotle Reports Suspicious Activity on POS System*, Infosecurity Magazine (Apr. 26, 2017), https://www.infosecurity-magazine.com/news/chipotle-suspicious-activity-pos/. (last visited Aug. 9, 2019)
[25] Brett Hawkins, Case Study: The Home Depot Data Breach at 3-4, (Jan. 2015), https://webcache.googleusercontent.com/search?q=cache:CVF71JrfkhcJ:https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367+&cd=1&hl=en&ct=clnk&gl=us (last visited Aug. 9, 2019).
[26] *Id*. at 4, 7.
[27] Brian Krebs, *1,025 Wendy's Locations Hit in Card Breach*, KrebsonSecurity (July 8, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/. (last visited Aug. 9, 2019)

hit the United States in the last several years.[28] In the last five years, practically every major data breach involving retail store chains has been the result of malware placed on POS systems. Accordingly, data security experts have warned companies, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[29] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[30] The amount of payment card data compromised by data breaches is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[31]

60. A 2016 report by Verizon confirmed the vast majority of successful breaches often leverage legitimate credentials to gain access to the POS environment, using malware such as a RAM scraper to capture payment card data.[32] According to Verizon, hackers successfully compromise POS systems in a matter of minutes or hours and exfiltrate data within days of placing malware on the POS devices.[33]

61. Intruders with access to unencrypted Track 1 and Track 2 payment card data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[34] Since 2014, malware

---

[28] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), available at https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last visited Aug. 9, 2019).

[29] Datacap Systems, Inc., *Point of sale security: Retail data breaches at a glance*, available at https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance# (last visited Aug. 9, 2019).

[30] *Id.*

[31] *A Special Report on Attacks*, *supra* note 18, at 3.

[32] *See, e.g.*, Verizon, *2016 Data Breach Investigations Report* at 21, 31 (Apr. 2016), available at https://regmedia.co.uk/2016/05/12/dbir_2016.pdf (last visited Aug. 9, 2019).

[33] *Id.* at 10.

[34] *A Special Report on Attacks*, *supra* note 18, at 3.

installed on POS systems has been responsible for nearly every major data breach of a retail outlet.[35] In 2015, intrusions into POS systems accounted for 64% of all breaches where intruders successfully stole data.[36]

62. Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, Defendants were aware or should have been aware of the need to safeguard their POS systems. Nonetheless, despite the well-known vulnerabilities of POS systems, there are security measures and business practices that would have significantly reduced or eliminated hackers' ability to successfully infiltrate Defendants' POS systems. One report indicated that over 90% of the data breaches occurring in 2017 were preventable.[37]

63. Certain data security organizations, federal agencies, and state governments have implemented recommended standards of care regarding security measures designed to prevent these types of intrusions into POS systems. Defendants' adherence to reasonable standards of care could have either prevented or timely detected this Security Breach.

64. Defendants' treatment of Private Information entrusted to them by their customers fell far short of satisfying their legal duties and obligations. Defendants failed to ensure that access to their data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings, and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

---

[35] *Id.*
[36] Verizon, *supra* note 32, at 25.
[37] Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* at 3, (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf. (last visited Aug. 9, 2019)

Defendants Failed to Comply with Industry Standards

65. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[38]

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which establishes guidelines for fundamental data security principles and practices for business.[39] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

67. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious

[38] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 9, 2019).
[39] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 9, 2019).

activity on the network; and verify that third-party service providers have implemented reasonable security measures.[40]

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. Defendant HBC affirmatively undertook responsibility for data security at Lord & Taylor and Saks retail stores. Defendants were at all times fully aware of their obligation to protect the Private Information of their customers because of their participation in payment card processing networks. Defendants were also aware of the significant repercussions if they failed to do so because they collected payment card data from thousands of customers daily at their stores and Defendants knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and Class members.

70. The payment card networks (MasterCard, Visa, Discover, and American Express), data security organizations, state governments, and federal agencies have all implemented various standards and guidance on security measures designed to prevent these types of intrusions into POS systems. However, despite Defendants' understanding of the risk of data theft via malware installed on POS systems, the widely available resources to prevent intrusion into POS data systems, and Defendants' previous public display of customer's private information, Defendants

[40] Federal Trade Commission, *Start With Security*, *supra* note 38.

failed to adhere to these guidelines and failed to take reasonable and sufficient protective measures to prevent the Security Breach.

71. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, Symantec recommends "point to point encryption" implemented through secure card readers, which encrypts credit card information in the POS system, preventing malware that extracts card information through the POS memory while it processes the transaction.[41] Moreover, Symantec emphasized the importance of adopting EMV chip technology. Datacap Systems, a developer of POS systems, also recommends similar preventative measures.[42]

72. The major payment card industry brands set forth specific security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

73. 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.[43]

[41] *A Special Report on Attacks*, *supra* note 18, at 6.
[42] *See* Datacap Systems, *supra* note 29.
[43] *Payment Card Industry Data Security Standard* v3.2, at 5 (Apr. 2016), *available at* https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited Aug. 9, 2019).

74. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[44] PCI DSS sets the minimum level of what must be done, not the maximum.

75. PCI DSS 3.2, the version of the standards in effect at the time of the Security Breach, imposes the following mandates on Defendants:[45]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

76. Among other things, PCI DSS required Defendants to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

77. PCI DSS also required Defendants to not store "the full contents of . . . the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[46]

78. Despite Defendants' awareness of their data security obligations and their promises to customers that their personal data would be secured and protected, Defendants' treatment of

[44] *Id.*
[45] *Id.*
[46] *Id.* at 38 (PCI DSS 3.2.1 and 3.2.2).

Private Information entrusted to them by their customers fell far short of satisfying Defendants' legal duties and obligations, and included violations of the PCI DSS. Defendants failed to ensure that access to their data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

79. As a result of Defendants' failure to adhere to industry and government standards for the security of card data, Private Information of thousands of Defendants' customers, including Plaintiffs and Class members, was compromised over a time period spanning nearly one year.

Defendants Promised to Protect Customers' PI, but Maintained Inadequate Data Security

80. Prior to and during the Security Breach, HBC, on behalf of its affiliated companies, promised its customers whose PI it collects that it would make every effort to protect their PI. Saks' and Lord & Taylor's privacy policies, drafted in part by HBC in New York and made available on Defendants' websites, describes the types of PI HBC collects from customers who visit its website, use their mobile applications and visit or make a purchase at one of their stores. Saks' privacy policy, updated May 2018, stated, in relevant part:

> We have taken certain physical, administrative, and technical steps to safeguard the information we collect from and about our customers and Site visitors. While we make every effort to help ensure the integrity and security of our network and systems, we cannot guarantee our security measures. When you enter sensitive information (such as credit card information) on our forms, we encrypt the transmission of that information using secure socket layer technology (SSL).[47]

81. Lord & Taylor's privacy policy, stated, in relevant part:

> We have taken certain physical, administrative, and technical steps to safeguard the information we collect from and about our customers and Site visitors. While we make every effort to help ensure the integrity and security of our network and systems, we cannot guarantee our security measures. When you enter sensitive

[47] https://www.saksfifthavenue.com/Policies#faq09 (last visited Aug. 9, 2019).

> information (such as credit card information) on our forms, we encrypt the transmission of that information using secure socket layer technology (SSL).[48]

82. In fact, prior to the Security Breach at issue in this action, Saks had made even more assurances to its customers which have proved to be baseless, when it stated in its security policies on its website as late as January 2016 that:

> Protecting the security of your information is very important to us. When you transmit sensitive personal information (such as credit card information) from your computer to our servers, your information is protected by both a "firewall" (a combination of computer hardware and software that helps keep unauthorized visitors from accessing information within our computer network) and industry standard SSL (secure socket layer) encryption. For our mobile website, we protect your payment card information using encryption technology when you place an order. Once we receive your transmission, we will take reasonable precautions to secure and protect the information on our systems. Unfortunately, no data transmission over the Internet can be 100% secure and, accordingly, we cannot guarantee or warrant the security of any information you disclose or transmit to us online. However, we strive to protect your information and privacy.[49]

Security Breaches Lead to Identity Theft

83. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[50]

84. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity

[48] http://web.archive.org/web/20170922064212/http://www.lordandtaylor.com:80/Policies#infoltcollect (last visited Aug. 9, 2019).

[49] http://web.archive.org/web/20140821045613/http://www.saksfifthavenue.com/Policies#sakssecurity (last visited Aug. 9, 2019).

[50] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf. (last visited Aug. 9, 2019).

thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[51]

85. Private Information—which includes Plaintiffs' and Class members' names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action—is a valuable commodity to identity thieves. Indeed, at all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Private Information they maintain is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud as stolen Private Information is a valuable commodity. A "cyber black-market", such as the one used by JokerStash, exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. The Private Information is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

86. Legitimate organizations and the criminal underground alike recognize the value in Private Information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. Plaintiffs' and Class members' personal information is being sold and traded by cyber criminals on the dark web. Criminals often trade the information on the dark web for a number of years.

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

87. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use.[52] Private information that is "linked" or "linkable" is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information the NIST report cites is a Massachusetts Institute of Technology study showing that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

88. Private information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

The Monetary Value of Privacy Protections and Private Information

89. The fact that Plaintiffs' and Class members' Private Information was stolen in order to be sold on the dark web—and is presently offered for sale to cyber criminals on the dark web—demonstrates the monetary value of the Private Information.

90. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

---

[52] Erika McCallister, *et al.*, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology Special Publication 800-122, 3-3, available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990 (last visited Aug. 9, 2019).

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[53]

91. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[54]

92. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[55]

93. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[56] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a

---

[53] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001) available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf. (last visited Aug. 9, 2019).

[54] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html. (last visited Aug. 9, 2019).

[55] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf. (last visited Aug. 9, 2019).

[56] *Web's Hot New Commodity: Privacy*, *supra* note 54.

profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

94. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[57]

95. The value of Plaintiffs' and Class members' Private Information on the black market is substantial, ranging from $1.50 to $90 per card number.[58]

96. Despite being aware of the value criminals attach to such Private Information, Defendants failed to sufficiently invest in their data security practices. Rather, with its "soaring profits and revenues", Defendants heavily invested in the remodeling of their stores and upgrades to its distribution and fulfillment centers, with "[o]ne of the company's biggest initiatives (accounting for 30% of the growth initiative budget) involves expanding the retail portfolio of its Saks Fifth Avenue division with seven full-line Saks stores and 32 new Saks OFF 5th off-price stores."[59] "Another 30% of the growth budget" is spent on investments such as "the robotic automatic of the company's distribution center in Toronto and a new e-commerce fulfillment center in the U.S."[60] Despite these substantial investments to upgrade the appearance and technology of their stores to boost sales, Defendants failed to make meaningful improvements to

---

[57] *See* DOJ, *Victims of Identity Theft, 2014*, *supra* note 50, at 6.
[58] Leapfrog, *The Cyber Black Market: What's Your Bank Login Worth* (Mar. 1, 2011), available at https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/. (last visited Aug. 9, 2019)
[59] Mike Troy, *Surging Hudson's Bay Details Major Investments in Expanding Saks, Saks Off 5th and Store Renovations*, Chain Store Age (Apr. 5, 2016), available at https://www.chainstoreage.com/article/surging-hudsons-bay-details-major-investments-expanding-saks-saks-th-and-store-renovations/. (last visited Aug. 9, 2019)
[60] *Id.*

their data security systems, including their POS systems, placing customer's Private Information at risk.[61]

97. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Private Information they maintain is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendants should have particularly been aware of these risks given the significant volume of daily credit and debit card transactions at their North American retail locations, amounting to a large volume of daily payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

98. Defendants had the resources to prevent a breach, particularly considering the aforementioned expansions in Defendants' retail locations and investments in technology. Defendants neglected to adequately invest in data security, despite the growing number of POS intrusions and several years of well-publicized data breaches.[62]

99. Had Defendants remedied the deficiencies in their POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Defendants would have prevented intrusion into their POS systems and, ultimately, the theft of their customers' confidential payment card information.

---

[61] On information and belief, Defendants contracted with various third parties to install, manage, service and maintain the POS equipment and software. These third parties may also be responsible or liable for allowing the hackers to gain access and deploy malware on the POS systems in Defendants' network. Plaintiffs hereby provide notice that after discovery, they may seek leave to add those third-party vendors as party defendants in this litigation.

[62] Mike Troy, *supra* note 59.

100. Given these facts, any company that transacts business with consumers and then compromises the privacy of consumers' Private Information has thus deprived consumers of the full monetary value of their transaction with the company.

Damages Sustained by Plaintiffs and Class Members

101. A portion of the services purchased from Defendants by Plaintiffs and the other Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of Private Information, including their credit and debit card information. The cost to Defendants of collecting and safeguarding Private Information is built into the price of all of their services. Because Plaintiffs and the other Class members were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the other Class members incurred actual monetary damages in that they overpaid for their purchases at Saks and Lord & Taylor stores.

102. Plaintiffs and the other members of the Class have suffered additional injury and damages, including, but not limited to one or more of the following:

a. unauthorized use of their PI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PI;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills

and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

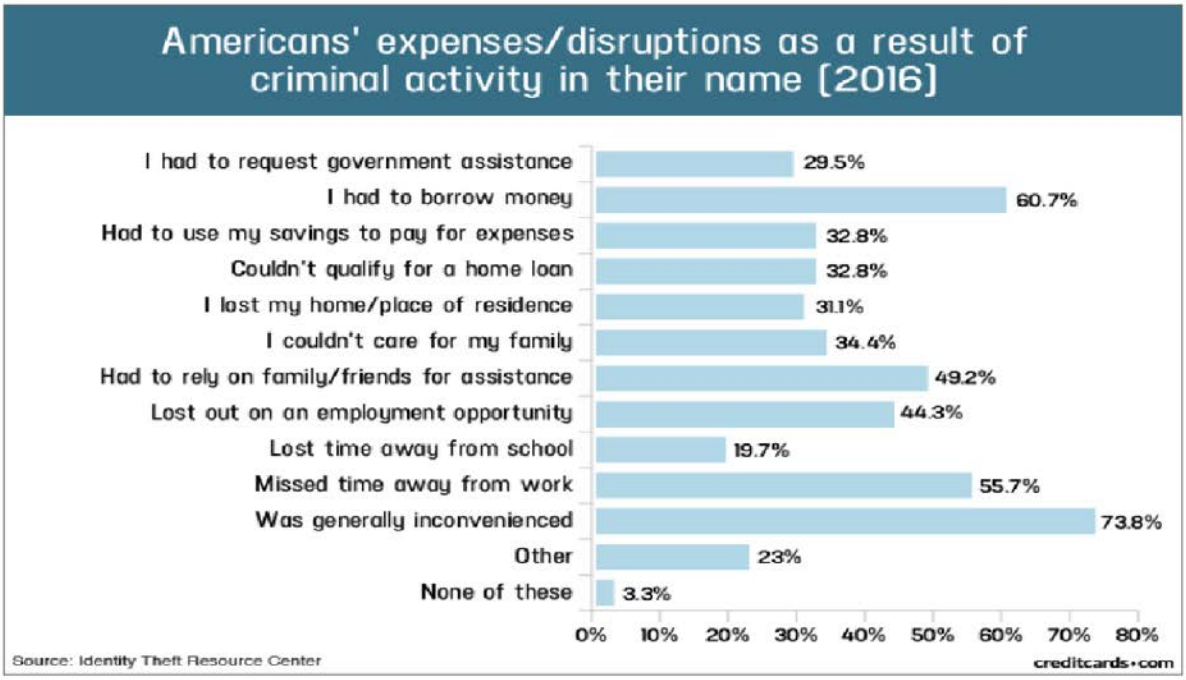
f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Security Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach;

g. the imminent and impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;

h. damages to and diminution in value of their PI entrusted to Defendants for the sole purpose of purchasing products and services from Saks and Lord & Taylor; and the loss of Plaintiffs' and Class members' privacy.

103. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal information:[63]

[63] Jason Steele, Credit Card and ID Theft Statistics (Oct. 24, 2017) available at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited Aug. 9, 2019)



104. Acknowledging the damage to Plaintiffs and Class members, Defendants instructed customers who used their card at their stores to take certain cautionary steps. Credit and debit card users were told they should review their accounts for unauthorized transactions and notify their banks immediately if they discover any unauthorized purchases or cash advances. Plaintiffs and the other Class members now face a greater risk of identity theft.

V. CLASS ACTION ALLEGATIONS

105. Plaintiffs bring all counts, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Nationwide Class defined as:

> All persons who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, or Lord & Taylor store during the period from May 1, 2017 through April 1, 2018.

106. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims under the laws of the individual States, and on behalf of separate State Subclasses, defined as follows:

All persons residing in Arizona and non-residents, who used their credit, debit, or prepaid debit card at a Saks and/or Saks OFF 5TH store in Arizona during the period from May 1, 2017 through April 1, 2018 (the "Arizona Subclass").

All persons residing in California and non-residents, who used their credit, debit, or prepaid debit card at a Saks and/or Saks OFF 5TH store in California during the period from May 1, 2017 through April 1, 2018 (the "California Subclass").

All persons residing in Connecticut and non-residents, who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, and/or Lord & Taylor store in Connecticut during the period from May 1, 2017 through April 1, 2018 (the "Connecticut Subclass").

All persons residing in Florida and non-residents, who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, and/or Lord & Taylor store in Florida during the period from May 1, 2017 through April 1, 2018 (the "Florida Subclass").

All persons residing in Illinois and non-residents, who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, and/or Lord & Taylor store in Illinois during the period from May 1, 2017 through April 1, 2018 (the "Illinois Subclass").

All persons residing in Kentucky and non-residents, who used their credit, debit, or prepaid debit card at a Saks and/or Saks OFF 5TH store in Kentucky during the period from May 1, 2017 through April 1, 2018 (the "Kentucky Subclass").

All persons residing in New Jersey or non-residents, who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, and/or Lord & Taylor store in New Jersey during the period from May 1, 2017 through April 1, 2018 (the "New Jersey Subclass").

All persons residing in New York and non-residents, who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, and/or Lord & Taylor store in New York during the period from May 1, 2017 through April 1, 2018 (the "New York Subclass").

All persons residing in Pennsylvania and non-residents, who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, and/or Lord & Taylor store in Pennsylvania during the period from May 1, 2017 through April 1, 2018 (the "Pennsylvania Subclass").

All persons residing in Texas and non-residents, who used their credit, debit, or prepaid debit card at a Saks, Saks OFF 5TH, store

in Texas during the period from May 1, 2017 through April 1, 2018 (the "Texas Subclass").

107. Excluded from the Class and Subclasses are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

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

109. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class and Subclasses are so numerous that joinder of all Class members would be impracticable. On information and belief, Class and Subclass members number in the tens if not hundreds of thousands.

110. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class and Subclass members and predominate over questions affecting only individual Class and Subclass members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class and Subclass members' Private Information;

b. Whether Defendants properly implemented their purported security measures to protect Plaintiffs' and Class and Subclass members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether Defendants took reasonable measures to determine the extent of the Security Breach after they first learned of same;

d. Whether Defendants disclosed Plaintiffs' and Class and Subclass members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

e. Whether Defendants' conduct constitutes breach of an implied contract;

f. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class and Subclass members' Private Information;

g. Whether Defendants were negligent in failing to properly secure and protect Plaintiffs' and Class and Subclass members' Private Information;

h. Whether Plaintiffs and the other members of the Class and Subclasses are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

111. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Class and Subclass members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

112. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class and Subclass members because, among other things, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiffs.

113. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class and Subclass representatives because their interests do not conflict with the interests of the other Class and Subclass members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class' and Subclasses' interests will be fairly and adequately protected by Plaintiffs and their counsel.

114. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted and/or refused to act on grounds that apply generally to the Class and Subclasses, making injunctive and/or declaratory relief appropriate with respect to the classes under Fed. Civ. P. 23 (b)(2).

115. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class and Subclass members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class and Subclass members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the State Subclasses)

116. Plaintiffs repeat and re-allege Paragraphs 1 through 115 as if fully set forth herein.

117. Upon accepting and storing the Plaintiffs' and Class members' PI in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the PI was private and confidential and should be protected as private and confidential.

118. Defendants owed a duty of care not to subject Plaintiffs' and Class members' PI to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

119. Defendants owed numerous duties to Plaintiffs and Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PI in their possession;
b. to protect PI using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

120. Defendants also breached their duty to Plaintiffs and Class members to adequately protect and safeguard PI by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PI. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the PI with which they were and are entrusted, in spite of the known risk and

foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' PI, misuse the PI and intentionally disclose it to others without consent.

121. Defendants knew, or should have known, of the risks inherent in collecting and storing PI, the vulnerabilities of POS systems, and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches within the retail industry, including their own security failures in the March 2017 public disclosure of customer's private information and Defendants' previous admissions.

122. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PI.

123. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PI.

124. Because Defendants knew that a breach of their systems would damage millions of their customers, including Plaintiffs and Class members, Defendants had a duty to adequately protect their data systems and the PI contained thereon.

125. Defendants had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Defendants with their PI was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems, and the PI they stored on them, from attack.

126. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PI. Defendants' misconduct included failing to: (1) secure their point-of-sale systems, despite knowing their vulnerabilities; (2) comply with industry standard security

practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

127. Defendants also had independent duties under state and federal laws that required them to reasonably safeguard Plaintiffs' and Class members' PI and promptly notify them about the Security Breach.

128. Defendants breached their duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PI;
b. by creating a foreseeable risk of harm through the misconduct previously described;
c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' PI both before and after learning of the Security Breach;
d. by failing to comply with the minimum industry data security standards during the period of the Security Breach; and
e. by failing to timely disclose that Plaintiffs' and Class members' PI had been improperly acquired or accessed.

129. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiffs' and Class members' PI from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PI during the time it was within Defendants' possession or control.

130. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PI to Plaintiffs and the Class members so that they can take

appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PI.

131. Defendants further breached their statutory duties designed to protect the public from harms caused by data breaches, including but not limited to duties to use reasonable measures to protect PI imposed by Section 5 of the FTC Act.

132. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect Plaintiffs' and Class members' PI from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PI during the time it was within Defendants' possession or control.

133. Further, through their failure to discover the breach for approximately one year, Defendants prevented Plaintiffs and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

134. Upon information and belief, Defendants improperly and inadequately safeguarded Plaintiffs' and Class members' PI in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendants' failure to take proper security measures to protect Plaintiffs' and Class members' sensitive Customer Data, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the PI.

135. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PI; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons

having access to Plaintiffs' and Class members' PI; and failing to provide Plaintiffs and Class members with timely notice that their sensitive PI had been compromised.

136. Neither Plaintiffs nor the other Class members contributed to the Security Breach and subsequent misuse of their PI as described in this Complaint.

137. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the State Subclasses)

138. Plaintiffs repeat and re-allege Paragraphs 1 through 115 as if fully set forth herein.

139. Defendants solicited and invited Plaintiffs and Class members to shop at their retail stores and make purchases using their credit or debit cards. Plaintiffs and Class members accepted Defendants' offers and used their credit or debit cards to make purchases at Defendants' stores.

140. When Plaintiffs and Class members made and paid for purchases of Defendants' services and products, they provided their PI to Defendants. In so doing, Plaintiffs and Class members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely detect any breaches of their PI.

141. Plaintiffs and Class members would not have provided and entrusted their PI with Defendants in the absence of the implied contract between them and Defendants.

142. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

143. Defendants breached the implied contracts they made with Plaintiffs and Class members by failing to safeguard and protect their PI and by failing to timely detect the data breach within a reasonable time.

144. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants, Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail above.

COUNT III
Unjust Enrichment/Quasi-Contract
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the State Subclasses)

145. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

146. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and provided Defendants with their payment information. In exchange, Plaintiffs and Class members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their PI with adequate data security.

147. Defendants knew that Plaintiffs and Class members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendants profited from Plaintiffs' purchases and used Plaintiffs' and Class members' PI for business purposes.

148. Defendants failed to secure Plaintiffs' and Class members' PI and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' PI provided.

149. Defendants acquired the PI through inequitable means as they failed to disclose the inadequate security practices previously alleged.

150. If Plaintiffs and Class members knew that Defendants would not secure their PI using adequate security, they would not have made purchases at Defendants' stores.

151. Plaintiffs and Class members have no adequate remedy at law.

152. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

153. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class members overpaid.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the State Subclasses)

154. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

155. At all times during Plaintiffs' and Class members' interactions with Defendants, Defendants were fully aware of the confidential, novel, and sensitive nature of Plaintiffs' and Class members' Private Information that Plaintiffs and Class members provided to Defendants.

156. As alleged herein and above, Defendants' relationship with Plaintiffs and Class members was governed by expectations that Plaintiffs' and Class members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

157. Plaintiffs and Class members provided their respective Private Information to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the Private Information to be disseminated to any unauthorized parties.

158. Plaintiffs and Class members also provided their respective Private Information to Defendants with the explicit and implicit understanding that Defendants would take precautions

to protect that Private Information from unauthorized disclosure, such as following basic principles of information security practices.

159. Defendants voluntarily received in confidence Plaintiffs' and Class members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

160. Due to Defendant's failure to prevent, detect, and/or avoid the Security Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class members' Private Information, Plaintiffs' and Class members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

161. But for Defendants' disclosure of Plaintiffs' and Class members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Security Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' Private Information, as well as the resulting damages.

162. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class members' Private Information. Defendants knew their computer systems and technologies for accepting and securing Plaintiffs' and Class members' Private Information had numerous security vulnerabilities because Defendants failed to observe industry standard information security practices.

163. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT V
Violation of Arizona Consumer Fraud Act
Ariz. Rev. Stat. § 44-1521, *et seq*.
(Asserted by Plaintiff Knight on behalf of the Arizona Subclass)

164. Plaintiff Knight ("Plaintiff," for purposes of this Count), individually and on behalf of the other Arizona Subclass members, repeats and re-alleges the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

165. Defendants, while operating in Arizona, used and employed deception, deceptive and unfair acts and practices, fraud, misrepresentation, and the concealment, suppression, and omission of material facts with the intent that others rely on such concealment, suppression and omission, in connection with the sale and advertisement of services, in violation of Ariz. Rev. Stat. § 44- 1522(A). This includes but is not limited to the following:

a. Defendants failed to enact adequate privacy and security measures to protect the Arizona Subclass members' PI from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Security Breach;

b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Security Breach;

c. Defendants knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard Arizona Subclass members' PI from unauthorized disclosure, release, data breaches, and theft;

d. Defendants knowingly omitted, suppressed, and concealed the inadequacy of their privacy and security protections for the Arizona Subclass members' PI;

e. Defendants knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Arizona Subclass members' PI;

f. Defendants failed to maintain the privacy and security of Arizona Subclass members' PI, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Security Breach; and

g. Defendants failed to disclose the Security Breach to the Arizona Subclass members in a timely manner, in violation of Ariz. Rev. Stat. § 44-7501, et seq.

166. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Arizona Subclass that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

167. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff's and the Arizona Subclass members' PI and that the risk of a data breach or theft was highly likely. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Arizona Subclass.

168. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

169. Plaintiff and the Arizona Subclass seek monetary relief against Defendants in an amount to be determined at trial.

170. Plaintiff and the Arizona Subclass also seek an order enjoining Defendants' unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Arizona Consumer Fraud Act, Arizona Rev. Stat. § 44- 1522, *et seq*.

COUNT VI
Violations of California Unfair Competition Law
Cal. Bus. And Prof. Code § 17200, *et seq.*
(Asserted by Plaintiffs Rudolph and Vains on behalf of the California Subclass)

171. Plaintiffs Rudolph and Vains ("Plaintiffs," for purposes of this Count), individually and on behalf of the other California Subclass members, repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

172. UCL § 17200 provides, in pertinent part, that "unfair competition shall mean and include unlawful, unfair, or fraudulent business practices [. . .]".

173. Under the UCL, a business act or practice is "unlawful" if the act or practice violates any established state or federal law.

174. Defendants' failures to implement and maintain reasonable security measures and to timely and properly notify Plaintiffs and Class members of the Security Breach therefore was and continues to be "unlawful" as Defendants breached their implied and express warranties and violated the California law regarding data breaches, including but not limited to Cal. Civ. Code § 1798.81.5 and Section 5 of the FTC Act.

175. As a result of Defendants' unlawful business acts and practices, Defendants unlawfully obtained money from Plaintiffs and Class members.

176. Under the UCL, a business act or practice is "unfair" if the defendant's conduct is substantially injurious to consumers, goes against public policy, and is immoral, unethical, oppressive, and unscrupulous, as the benefits for committing these acts or practices are outweighed by the severity of the harm to the alleged victims.

177. Defendants' conduct alleged herein was and continues to be of no benefit to their customers, as it is both injurious and unlawful to those persons who rely on Defendants' duties and obligations to maintain and implement reasonable data security measures and to monitor for breaches. Having lax data security measures that has resulted in the disclosure of millions of customers' payment card information provides no benefit to consumers. For these reasons, Defendants' conduct was and continues to be "unfair" under the UCL.

178. As a result of Defendants' unfair business acts and practices, Defendants have unfairly and unlawfully obtained money from Plaintiffs and members of the Class.

179. Further, Defendants have fraudulently omitted material information in violation of the UCL by failing to disclose their inadequate data security measures, which was material to consumers as they would not have purchased items from Defendants' stores had Defendants disclosed the information. Further, Defendants had a duty to disclose this information to Plaintiffs and members of the California Subclass based on the factual allegations discussed herein, which demonstrate the following: (1) Defendants, Plaintiffs, and California Subclass members were in a special relationship arising from Defendants' role in safeguarding consumers' sensitive consumer data; (2) Defendants held exclusive knowledge of the material facts surrounding their inadequate data security measures, which were not known to Plaintiffs and class members; and (3) Defendants made a partial misrepresentation when warranting on their website that customers' private data would be secured, suppressing the material fact that their data security measures were inadequate.

180. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

181. Plaintiffs request that this Court enjoin Defendants from violating the UCL or violating the UCL in the same way in the future, as discussed herein. Otherwise, Plaintiffs and

members of the Class may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

COUNT VII
Violations of California Consumers Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq*.
(Asserted by Plaintiffs Rudolph and Vains on behalf of the California Subclass)

182. Plaintiffs Rudolph and Vains ("Plaintiffs," for purposes of this Count), individually and on behalf of the other California Subclass members, repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

183. The Consumers Legal Remedies Act, California Civil Code § 1750, *et seq*. (the "CLRA") has adopted a comprehensive statutory scheme prohibiting various deceptive practices in connection with the conduct of a business providing goods, property, or services to consumers primarily for personal, family, or household purposes. The self-declared purposes of the CLRA are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection.

184. Defendants are each a "person" as defined by Civil Code Section 1761(c), because Defendants are corporations as set forth above.

185. Plaintiffs and California Subclass members are "consumers" within the meaning of Civil Code Section 1761(d).

186. Defendants performed "services," as defined by California Civil Code Section 1761(a), with respect to their compilation, maintenance, use, and furnishing of Plaintiffs' and California Subclass members' PI that was compromised in the Security Breach.

187. Defendants' sale of their services constitutes "transaction[s]" which were "intended to result or which result[ed] in the sale" of services to consumers within the meaning of Civil Code Sections 1761(e) and 1770(a).

188. Plaintiffs have standing to pursue this claim as they suffered injury in fact and lost money as a result of Defendants' actions as set forth herein. Specifically, Plaintiffs' PI has been compromised and they are imminently threatened with financial and identity theft, and, in fact, many California Subclass members have already suffered actual fraud.

189. Section 1770(a)(5) of the CLRA prohibits anyone from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." Defendants represented that they would adequately secure Plaintiffs' and California Subclass members' PI when in fact their computer systems were inadequately protected and susceptible to breach.

190. Section 1770(a)(7) of the CLRA prohibits anyone from "[r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another." Defendants represented that they would adequately secure Plaintiffs' and California Subclass members' PI when in fact their computer systems were inadequately protected and susceptible to breach.

191. Section 1770(a)(9) of the CLRA prohibits anyone from "[a]dvertising goods or services with intent not to sell them as advertised." As noted above, Defendants failed to provide adequate security to the PI they were entrusted to secure.

192. Plaintiffs, individually and on behalf of the California Subclass, seek, at this time, monetary damages, injunctive relief, an order enjoining the acts and practices described above, and attorneys' fees, costs and expenses under the CLRA. On July 11, 2019, Plaintiff Vains sent a pre-suit demand letter to Defendants providing them with written notice of their alleged violations of the CLRA pursuant to California Civil Code section 1782(a) and requested that Defendants correct or agree to correct the violations enumerated and reimburse Plaintiff Vains and the

California Subclass for any damages suffered. By letter dated August 7, 2019, Defendants failed to provide Plaintiff Vains and the California Subclass with the full relief sought. As a direct and proximate cause of Defendants' conduct, Plaintiffs and California Subclass members suffered damages as alleged above and seek compensatory, monetary damages and punitive damages, in addition to injunctive and equitable relief.

COUNT VIII
Violation of The California Customer Records Act
(Asserted by Plaintiffs Rudolph and Vains on behalf of the California Subclass)

193. Plaintiffs Rudolph and Vains ("Plaintiffs," for purposes of this Count), individually and on behalf of the other California Subclass members, repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

194. The Security Breach described above constituted a "breach of the security system" of Defendants, within the meaning of Section 1798.82(g) of the California Civil Code.

195. Cal Civ. Code § 1798.81.5(a)(1) provides that its purpose is to "ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

196. Cal. Civ. Code § 1798.81.5(b) provides, in pertinent part, that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

197. The information acquired by criminals in the Security Breach constituted "personal information" within the meaning of Section 1798.80(e) of the California Civil Code.

198. Under Cal Civ. Code § 1798.81.5(d)(1)(A)(i-iv), "personal information," as described in Cal Civ. Code § 1798.81.5(b), means the following:

> (A) [a]n individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
> (i) Social security number.
> (ii) Driver's license number or California identification card number.
> (iii) Account number, ***credit or debit card number***, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
> (emphasis added)

199. Therefore, the Private Information disclosed in Defendants' Security Breach, which includes Plaintiffs and the California Subclass members' credit and debit card information, combined with the necessary codes and/or passwords, falls within the meaning of "personal information" under Cal. Civ. Code Section 1798.81.5.

200. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Security Breach.

201. Defendants unreasonably delayed informing anyone about the breach of security of Plaintiffs' and the California Subclass' confidential and non-public information after Defendants knew the Security Breach had occurred.

202. Defendants failed to disclose to the Plaintiffs and the California Subclass, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PI when they knew or reasonably believed such information had been compromised.

203. Upon information and belief, no law enforcement agency instructed Defendants that notification to Plaintiffs and the California Subclass would impede investigation.

204. As a result of Defendants' violation of Cal. Civ. Code § 1798.80 *et seq.*, Plaintiffs and the California Subclass incurred economic damages, including expenses associated with necessary credit monitoring.

205. Plaintiffs, individually and on behalf of the California Subclass, seek all remedies available under Cal. Civ. Code § 1798.84, including but not limited to: (a) damages suffered by the California Subclass as alleged above; (b) statutory damages for Defendants' willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief.

206. Plaintiffs, individually and on behalf of the California Subclass, also seek reasonable attorneys' fees and costs under Cal. Civ. Code § 1798.84(g).

COUNT IX
Violation of Connecticut's Unfair Trade Practices Act,
Conn. Gen. Stat. § 42-l10a, *et seq*. ("CUTPA")
(Asserted by Plaintiff Harris on behalf of the Connecticut Subclass)

207. Plaintiff Julia A. Harris ("Plaintiff," for purposes of this Count), individually and on behalf of the other Connecticut Subclass members, repeats and re-alleges the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

208. Defendants and their agents are engaged in trade and commerce in Connecticut.

209. Defendants and their agents engaged in deceptive, unfair and oppressive acts or practices by failing to disclose and/or misleading the Plaintiff and the Connecticut Subclass into providing Defendants and their agents with the PI, when Defendants and their agents knew or were reckless in not knowing that their computer systems were vulnerable to attack by hackers, and in fact were then presently under attack by hackers.

210. Plaintiff and the Connecticut Subclass entrusted Defendants and their agents with their PI.

211. As alleged herein in this Complaint, Defendants and their agents engaged in

unfair, deceptive, and oppressive acts or practices in the conduct of consumer transactions, including violations of CUTPA, by their:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PI;

c. failure to disclose that their computer systems and data security practices were inadequate to safeguard credit and debit card information and other PI from theft;

d. failing to detect the Security Breach in a timely fashion;

e. continued acceptance of PI and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Security Breach;

f. allowing unauthorized persons to have access to and make unauthorized charges to their customers' credit and/or debit card accounts.

212. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PI of Plaintiff and the Connecticut Subclass, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

213. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

214. Also as a direct result of Defendants' knowing violation of the CUTPA, Plaintiff Harris and the Connecticut Subclass are entitled to damages as well as equitable and injunctive relief, including, but not limited to:

a. ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

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

e. ordering that Defendants purge, delete, and destroy in a reasonably secure manner PI not necessary for their provisions of services;

f. ordering that Defendants conduct regular database scanning and security checks;

g. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal

information to third parties, as well as the steps Defendants' customers must take to protect themselves.

215. Plaintiff Harris brings this action on behalf of herself and the Connecticut Subclass for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Connecticut Subclass and the public from Defendants' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

COUNT X
Violation of Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. § 501.201, *et seq.*
(Asserted by Plaintiff Lefkowitz on behalf of the Florida Subclass)

216. Plaintiff Lefkowitz ("Plaintiff," for purposes of this Count), individually and on behalf of the other Florida Subclass members, repeats and re-alleges the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

217. At all relevant times, Plaintiff and Florida Subclass members were "consumers" within the meaning of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat § 501.201 *et seq.* ("FDUTPA").

218. Defendants are engaged in trade and commerce in Florida.

219. Plaintiff and the Florida Subclass entrusted Defendants with their PI.

220. As alleged in this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the FDUTPA:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PI;

c. failure to disclose that their computer systems and data security practices were inadequate to safeguard credit and debit card information and other PI from theft;

d. failing to detect the Security Breach in a timely fashion;

e. continued acceptance of PI and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Security Breach; and

f. allowing unauthorized persons to have access to and make unauthorized charges to their customers' credit and/or debit card accounts.

221. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PI of Plaintiff and Florida Subclass members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

222. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

223. As a direct result of Defendants' knowing violation of FDUTPA, Plaintiff and the Florida Subclass are entitled to damages as well as injunctive relief, including, but not limited to:

a. ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

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

d. ordering that Defendants purge, delete, and destroy in a reasonably secure manner PI not necessary for their provisions of services;

e. ordering that Defendants conduct regular database scanning and security checks;

f. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

g. ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps their customers must take to protect themselves.

224. Plaintiff brings this action on behalf of herself and Florida Subclass members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and Florida Subclass members and the public from Defendants' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

225. Plaintiff and the Florida Subclass seek actual damages under Fla. Stat. § 501.211(2) and all fees, costs, and expenses allowed by law, including attorney's fees and costs, pursuant to Federal Rule of Civil Procedure 23 and Fla. Stat. §§ 501.2105 and 501.211, to be proven at trial.

COUNT XI
Violation of the Illinois Consumer Fraud Act
815 Ill. Comp. Stat. 505/1, *et seq.*
(Asserted by Plaintiff Moss on behalf of the Illinois Subclass)

226. Plaintiff Greta Moss ("Plaintiff," for purposes of this Count), individually and on behalf of the other Illinois Subclass members, repeats and re-alleges the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

227. Defendants, while operating in Illinois, used and employed unfair and deceptive acts and practices, including deception and misrepresentation, in the conduct of trade or commerce, and unfair acts and practices, fraud, misrepresentation, and the concealment, suppression, and omission of material facts with the intent that others rely on such concealment, suppression and omission, in connection with the sale and advertisement of services, in violation of 815 Ill. Comp. Stat. 505/2. This includes but is not limited to the following:

a. Defendants failed to enact adequate privacy and security measures to protect Plaintiff's and the Illinois Subclass members' PI from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Security Breach;

b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Security Breach;

c. Defendants knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's

and the Illinois Subclass members' PI from unauthorized disclosure, release, data breaches, and theft;

d. Defendants failed to detect the Security Breach in a timely fashion;

e. Defendants knowingly omitted, suppressed, and concealed the inadequacy of their privacy and security protections for Plaintiff and the Illinois Subclass members' PI;

f. Defendants knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and the Illinois Subclass members' PI;

g. Defendants failed to maintain the privacy and security of Plaintiff's and the Illinois Subclass members' PI, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Security Breach; and

h. Defendants failed to disclose the Security Breach to Plaintiff and the Illinois Subclass members in a timely manner, in violation of the duties imposed by 815 Ill. Comp. Stat. § 530/10(a).

228. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

229. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff's and the Illinois Subclass members' PI and that the risk of a data breach or theft was highly likely. Defendants' actions were negligent,

knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Illinois Subclass members.

230. As a direct and proximate cause of Defendants' conduct, Plaintiff and the Illinois Subclass members suffered damages as alleged above.

231. Plaintiff and the Illinois Subclass seek relief under 815 Ill. Comp. Stat. 505/10a, including but not limited to damages, restitution and punitive damages (to be proven at trial), injunctive relief, and/or attorneys' fees and costs.

COUNT XII
Violation of the Kentucky Computer Security Breach Notification Act
Ky. Rev. Stat. Ann. § 365.732, *et seq.*
(Asserted by Plaintiff Payne on behalf of the Kentucky Subclass)

232. Plaintiff Larry Payne ("Plaintiff," for purposes of this Count), individually and on behalf of the other Kentucky Subclass members, repeats and re-alleges the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

233. Defendants are required to notify Plaintiff and Kentucky Subclass members if they become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' PI) in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

234. Defendants are businesses that hold computerized data that includes personal information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

235. The Kentucky Plaintiff and Kentucky Subclass members' PI includes personal information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

236. Because Defendants were aware of a breach of their security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky

Subclass members' PI), Defendants had an obligation to disclose the Security Breach in a timely fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

237. Thus, by failing to disclose the Security Breach in a timely manner, Defendants violated Ky. Rev. Stat. Ann. § 365.732(2).

238. As a direct and proximate result of Defendants' violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and the Kentucky Subclass members suffered damages, as described above.

239. Plaintiff and the Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including, but not limited to actual damages.

COUNT XIII
Violation of New Jersey's Consumer Fraud Act
N.J. Stat. Ann. § 56:8-1, *et seq.* ("NJCFA")
(Asserted by Plaintiffs Tafet and Carthan on behalf of the New Jersey Subclass)

240. Plaintiffs Debbie Carthan and Hope Tafet ("Plaintiffs," for purposes of this Count), individually and on behalf of the other New Jersey Subclass members, repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

241. As alleged herein, Defendants, while operating in New Jersey, engaged in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56.8-2. This includes, but is not limited to the following:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PI;

c. failing to detect the Security Breach in a timely manner;

d. failure to disclose that their computer systems and data security practices were inadequate to safeguard credit and debit card information and other PI from theft;

e. continued acceptance of PI and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Security Breach; and

f. allowing unauthorized persons to have access to and make unauthorized charges to their customers' credit and/or debit card accounts.

242. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PI of Plaintiffs and New Jersey Subclass members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

243. As a direct and proximate cause of Defendants' conduct, Plaintiffs and New Jersey Subclass members suffered damages as alleged above.

244. As a direct result of Defendants' knowing violation of the NJCFA, Plaintiffs and New Jersey Subclass members are entitled to damages as well as injunctive relief, including, but not limited to:

a. ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

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

d. ordering that Defendants purge, delete, and destroy in a reasonably secure manner PI not necessary for their provisions of services;

e. ordering that Defendants conduct regular database scanning and security checks;

f. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

g. ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants customers must take to protect themselves.

245. Plaintiffs bring this action on behalf of themselves and the New Jersey Subclass for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs and the New Jersey Subclass and the public from Defendants' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

246. Plaintiffs and the New Jersey Subclass also seek actual damages, injunctive and/or other equitable relief and treble damages, and attorney's fees and costs pursuant to Federal Rule of Civil Procedure 23 and N.J. Stat. Ann. § 56:8-19.

COUNT XIV
New Jersey Consumer Security Breach Disclosure Act,
N.J. Stat. Ann. § 56:8-163, *et seq.*
(Asserted by Plaintiffs Tafet and Carthan on behalf of the New Jersey Subclass)

247. Plaintiffs Debbie Carthan and Hope Tafet ("Plaintiffs," for purposes of this Count), individually and on behalf of the other New Jersey Subclass members, repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

248. Under N.J. Stat. Ann. §§ 56, 8-163(b), "[A]ny business . . . that complies or maintains computerized records that include personal information on behalf of another business or public entity shall notify the business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

249. Defendants are businesses that compile or maintain computerized records that include personal information on behalf of another business under N.J. Stat. Ann. §§ 56, 8-163(b).

250. Plaintiffs' and New Jersey Subclass members' PI (including but not limited to names, addresses, and social security numbers) includes personal information covered under N.J. Stat. Ann. §§ 56, 8-163, et seq.

251. Because Defendants discovered a breach of their security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, Defendants had an obligation to disclose the data breach in a timely fashion as mandated under N.J. Stat. Ann. §§ 56, 8-163, *et seq*.

252. By failing to disclose the data breach in a timely manner, Defendants violated N.J. Stat. Ann. §§ 56, 8-163(b).

253. As a direct and proximate result of the Defendants' violations of N.J. Stat. Ann. § 56, 8-163(b), Plaintiffs and New Jersey Subclass members suffered the damages described above.

254. Plaintiffs and New Jersey Subclass members seek relief under N.J. Stat. Ann. §§ 56, 8-19, including but not limited to actual damages, attorneys' fees and costs, and injunctive relief.

COUNT XV
Violations of New York Consumer Law for Deceptive Acts and Practices
N.Y. Gen. Bus. Law § 349
(On Behalf of all Plaintiffs and the Nationwide Class or, Alternatively by Plaintiffs Sacklow, Targum, Dennis Meduri, Georgina Meduri, Bernadette Beekman, Levitt-Raschella, Cona and Joseph on behalf of the New York Subclass)

255. All Plaintiffs (or alternatively Plaintiffs Jeanne Sacklow, Dennis Meduri, Georgina Meduri, Beekman, Erika Targum, Leslie Levitt-Raschella, John Cona and Cassondra Joseph) ("Plaintiffs," for purposes of this Count), individually and on behalf of the Nationwide Class (or alternatively, on behalf of the other New York Subclass members), repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

256. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

257. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

258. Defendants stored Plaintiffs' and the Class members' PI in Defendants' electronic and consumer information databases. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the Class members' PI secure and prevented

the loss or misuse of Plaintiffs' and the Class members' PI. Defendants did not disclose to Plaintiffs and the Class members that their data systems were not secure.

259. Plaintiffs and the Class never would have provided their sensitive and personal PI if they had been told or knew that Defendants failed to maintain sufficient security to keep such PI from being hacked and taken by others, and that Defendants failed to maintain the information in encrypted form.

260. Defendants violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendants' many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and the Class members' PI.

261. Defendants also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiffs and the Class members of the Security Breach. If Defendants had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages related to the Security Breach.

262. Defendants' practices, acts, policies and course of conduct violate NYGBL § 349 in that:

a. Defendants actively and knowingly misrepresented or omitted disclosure of material information to Plaintiffs and the Class at the time they provided such PI that Defendants did not have sufficient security or mechanisms to protect PI;

b. Defendants failed to give timely warnings and notices regarding the defects and problems with their system(s) of security systems that they maintained to protect Plaintiffs' and the Class' PI. Defendants possessed prior knowledge of the inherent

defects in their IT systems and failed to address the same or to give timely warnings that there had been a Security Breach.

263. Plaintiffs and the Class were entitled to assume, and did assume, Defendants would take appropriate measures to keep their PI safe. Defendants did not disclose at any time that Plaintiffs' and the Class' PI was vulnerable to hackers because Defendants' data security measures were inadequate, and Defendants were the only one in possession of that material information, which they had a duty to disclose.

264. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendants have, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system they maintained and failed to reveal the Security Breach timely and adequately.

265. Members of the public were deceived by and relied upon Defendants' affirmative misrepresentations and failures to disclose.

266. Such acts by Defendants are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her PI to Defendants. Said deceptive acts and practices are material. The requests for and use of such PI in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

267. Defendants' wrongful conduct caused Plaintiffs and the Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PI materials by third parties and placing the Plaintiffs and the Class at serious risk for monetary damages.

268. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

269. In addition to or in lieu of actual damages, because of the injury, Plaintiffs and the Class seek statutory damages for each injury and violation which has occurred.

COUNT XVI
Violation of New York's Data Breach Laws – Delayed Notification
(N.Y. Gen. Bus. Law § 899-aa)
(Asserted by Plaintiffs Sacklow, Targum, Dennis Meduri, Georgina Meduri, Beekman, Levitt-Raschella, Cona and Joseph on behalf of the New York Subclass)

270. Plaintiffs Jeanne Sacklow, Erika Targum, Dennis Meduri, Georgina Meduri, Beekman, Leslie Levitt-Raschella, John Cona and Cassondra Joseph ("Plaintiffs," for purposes of this Count), individually and on behalf of the other New York Subclass members, repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

271. Section 899-aa(3) of NYGBL requires any "person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization."

272. Section 899(5) of NYGBL states:

> The notice required by this section shall be directly provided to the affected persons by one of the following methods:
>
> (a) written notice;
>
> (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

> (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
>
> (d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:
>
> (1) e-mail notice when such business has an e-mail address for the subject persons;
>
> (2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and
>
> (3) notification to major statewide media.

273. The Security Breach described in this Complaint constitutes a "breach of the security system" of Defendants.

274. As alleged above, Defendants unreasonably delayed informing Plaintiffs and the New York Subclass about the Security Breach, affecting the confidential and non-public Private Information of Plaintiffs and the New York Subclass after Defendants knew the Security Breach had occurred.

275. Defendants failed to disclose to Plaintiffs and the New York Subclass, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendants knew or reasonably believed such information had been compromised.

276. Defendants' ongoing business interests gave Defendants incentive to conceal the Security Breach from the public to ensure continued revenue.

277. Upon information and belief, no law enforcement agency instructed Defendants that notification to the Plaintiffs and the New York Subclass would impede Defendants' investigation.

278. As a result of Defendants' violation of New York law, Plaintiffs and the New York Subclass were deprived of prompt notice of the Security Breach and were thus prevented from taking appropriate protective measures, including closing their payment card accounts, not using payment cards as payment for merchandise at Saks or Lord & Taylor stores, securing identity theft protection, or requesting a credit freeze. These measures would have prevented some or all of the damages Plaintiffs and the New York Subclass suffered because their stolen information would not have any value to identity thieves.

279. As a result of Defendants' violation of New York law, Plaintiffs and the New York Subclass have suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

280. Plaintiffs and the New York Subclass seek all remedies available under New York law, including, but not limited to damages the Plaintiffs and the New York Subclass suffered as alleged above, as well as equitable relief.

COUNT XVII
Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law
UTPCPL 73 § 201-2 &202-3 *et seq.*
(Asserted by Plaintiffs McGurn and Haggarty on behalf of the Pennsylvania Subclass)

281. Plaintiffs McGurn and Haggarty ("Plaintiffs," for purposes of this Count), individually and on behalf of the other Pennsylvania Subclass members, repeat and re-allege the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

282. Defendants, Plaintiffs, and the Pennsylvania Subclass are "Person[s]" within the meaning of Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 PS § 201, et seq.

283. The Pennsylvania UTPCPL 73 PS § 201-3 declares unlawful "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce …."

284. Defendants' business acts and practices alleged herein constituted deceptive acts or practices under Pennsylvania UTPCPL 73 PS § 201, *et seq*.

285. Defendants engaged in deceptive acts or practices by engaging in the course of conduct described herein.

286. Defendants knew or should have known of vulnerabilities and defects in their data security systems storing PI of Plaintiffs and the Pennsylvania Subclass before the Security Breach but concealed that information in violation of the UTPCPL.

287. Defendants engaged in deceptive acts and practices by failing to disclose and actively concealing known data-security defects, and by otherwise deceiving the Plaintiffs and the Pennsylvania Subclass.

288. More specifically, Defendants engaged in deceptive trade practices by:

a. Misrepresenting or omitting material facts to Plaintiffs and the Pennsylvania Subclass regarding the adequacy of their data security procedures protecting PI in violation of 73 Pa. Cons. Stat. §201-3(4) (v), (vii), (ix) and (xxi);

b. Misrepresenting or omitting material facts to Plaintiffs and the Pennsylvania Subclass regarding their failure to comply with relevant state and federal laws designed to protect consumers' privacy and PI in violation of 73 Pa. Cons. Stat. §201-3(4)(v), (vii), (ix), and (xxi);

c. Failing to discover and disclose the Security Breach to Plaintiffs and the Pennsylvania Subclass in a timely manner in violation of 73 Pa. Cons, Stat §2303(a);

d. Engaging in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiffs' and the Pennsylvania Subclass' PI, in violation of duties imposed by public policies reflected in applicable federal and state laws, resulting in the Security Breach. These deceptive acts and practices were likely to and did deceive Plaintiffs and the Pennsylvania Subclass regarding the lack of security protecting their PI; and

e. Engaging in unfair, unlawful, and deceptive acts and practices by failing to take proper action following the Security Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Pennsylvania Subclass' PI from further unauthorized disclosure, release, data breaches, and theft.

289. Defendants intentionally and knowingly misrepresented such material facts with an intent to mislead the Plaintiffs and the Pennsylvania Subclass.

290. The above unlawful, unfair, and deceptive acts and practices by Defendants were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Plaintiffs and the Pennsylvania Subclass that they could not reasonably avoid, this substantial injury outweighed any benefits to consumers or to competition.

291. Defendants owed to Plaintiffs and the Pennsylvania Subclass a duty to disclose their data-security defects because Defendants possessed exclusive knowledge regarding the vulnerability of the PI, concealed the data security defects from Plaintiffs and the Pennsylvania

Subclass, and made incomplete representations regarding their data security systems while withholding material facts from Plaintiffs and the Pennsylvania Subclass.

292. These representations and omissions were material to Plaintiffs and the Pennsylvania Subclass due to the value and sensitivity of the PI.

293. Plaintiffs and the Pennsylvania Subclass suffered ascertainable loss as a result of Defendants' misrepresentations, concealment, and omissions of material information as alleged herein.

294. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

295. Plaintiffs and the Pennsylvania Subclass seek an order enjoining Defendants' deceptive acts and practices, and awarding attorneys' fees, and any other just and proper relief available under UTPCPL.

296. In addition to or in lieu of actual damages, Plaintiffs and the Pennsylvania Subclass seek statutory damages for each injury and violation which has occurred.

297. Plaintiffs and the Pennsylvania Subclass seek relief under 73 Pa. Cons. Stat.§201-9.2, including, but not limited to, injunctive relief, actual damages, or $100 per Pennsylvania Subclass member, whichever is greater, treble damages, and attorneys' fees and costs.

COUNT XVIII
Texas Deceptive Trade Practices and Consumer Protection Act,
Tex. Bus. & Com. Code § 17.41, *et seq.*
(Asserted by Plaintiff Wade on behalf of the Texas Subclass)

298. Plaintiff Mark Wade ("Plaintiff," for purposes of this Count), individually and on behalf of the other Texas Subclass members, repeats and re-alleges the allegations contained in paragraphs 1 through 115 as though fully set forth herein.

299. Defendants' business acts and practices alleged herein constitute unfair, unconscionable, and deceptive methods, acts, and practices under the Texas Deceptive Trade Practices and Consumer Protection Act, Tex. Bus. & Com. Code § 17.41 et seq. ("TDTPA").

300. At all relevant times, Plaintiff and the Texas Subclass were "consumers" within the meaning of the TDTPA.

301. Defendants' conduct, as set forth herein, occurred in the conduct of "trade or commerce" within the meaning of the TDTPA.

302. The practices of Defendants, described above, violate the TDTPA for, *inter alia*, one or more of the following reasons:

a. Defendants represented that goods or services have sponsorship, approval, characteristics, uses, and benefits that they do not have;

b. Defendants provided, disseminated, marketed, and otherwise distributed uniform false and misleading advertisements, technical data and other information to consumers regarding the security of PI;

c. Defendants engaged in unconscionable commercial practices in failing to reveal material facts and information about data security vulnerabilities, which did, or tended to, mislead Plaintiff and the Texas Subclass about facts that could not reasonably be known by the consumer;

d. Defendants failed to reveal facts that were material to the transactions in light of representations of fact made in a positive manner;

e. Defendants caused Plaintiff and the Texas Subclass to suffer a probability of confusion and a misunderstanding of legal rights, obligations and/or remedies by and through their conduct;

f. Defendants failed to reveal material facts to Plaintiff and the Texas Subclass with the intent that Plaintiff and the Texas Subclass rely upon the omission; and

g. Defendants made material representations and statements of fact to Plaintiff and the Texas Subclass that resulted in Plaintiff and the Texas Subclass reasonably believing the represented or suggested state of affairs to be other than what they actually were.

303. Defendants intended that Plaintiff and the Texas Subclass rely on their misrepresentations and omissions.

304. Defendants' actions impact the public interest because Plaintiff and the Texas Subclass were, and continue to be, injured in exactly the same way as thousands of others as a result of and pursuant to Defendants' generalized course of deception as described throughout the Complaint.

305. Plaintiff sent a demand for relief to Defendants on behalf of the Texas Subclass by letter dated September 14, 2018.

306. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

307. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

308. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff's and the Texas Subclass' PI and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named

unfair practices and deceptive acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Texas Subclass.

309. Plaintiff, individually and on behalf of the Texas Subclass, seeks relief under Tex. Bus. & Com. Code § 17.50, including, but not limited to, economic damages, treble damages, injunctive relief, restitution, and attorneys' fees and costs.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

A. Declaring that this action is a proper class action, certifying the Class and Subclasses as requested herein, designating Plaintiffs as Class and Subclass Representatives, and appointing Class Counsel as requested in Plaintiffs' expected motion for class certification;

B. Ordering Defendants to pay actual damages to Plaintiffs and the other members of the Class and Subclasses;

C. Ordering Defendants to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class and Subclasses;

D. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiffs and their counsel;

E. Ordering Defendants to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Date: August 9, 2019

Respectfully submitted,

/s/ Timothy J. Peter
Timothy J. Peter*
FARUQI & FARUQI, LLP
1617 JFK Boulevard, Ste. 1550
Philadelphia, PA 19103
Tel: (215) 277-5770
Fax: (215) 277-5771
tpeter@faruqilaw.com

Janine Pollack (JP 0178)
THE SULTZER LAW GROUP P.C.
351 W. 54th Street, Suite 1C
New York, New York 10019
Tel.: (212) 989-7810
Fax: (888) 749-7747
pollackj@thesultzerlawgroup.com

Interim Co-Lead Counsel for Plaintiffs and the Class

Christian Siebott
Nina Varindani
FARUQI & FARUQI, LLP
683 3rd Avenue, 26th Floor
New York, NY 10017
Tel: (212) 983-9330
Fax: (212) 983-9331
csiebott@faruqilaw.com
nvarindani@faruqilaw.com

Daniel Tepper
WOLF HALDENSTEIN ADLER

FREEMAN & HERZ LLP
270 Madison Avenue
New York, New York 10016
Tel.: (212) 545-4600
Fax: (212) 686-0114
tepper@whafh.com

Ben Barnow*
Erich P. Schork*
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

Howard T. Longman
Melissa R. Emert
STULL, STULL, & BRODY
6 East 45th Street
New York, NY 10017
Tel.: (212) 687-7230
Fax: (212) 490-2022
hlongman@ssbny.com
memert@ssbny.com

Charles E. Schaffer*
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cschaffer@lfsblaw.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, LPA
One West Fourth Street, 18th Floor
Cincinnati, OH 45202

Tel: (513) 345-8297
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

Gary Mason*
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Avenue NW
Suite 305
Washington, DC 20016
Tel: (202) 640-1168
Fax: (202) 429-2294
gmason@wbmllp.com

Laurence D. King
David A. Straite
Ralph E. Labaton
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue
New York, New York 10022
Tel: (212) 687-1980
Fax: (212) 687 7714
lking@kaplanfox.com
dstraite@kaplanfox.com
rlabaton@kaplanfox.com

John A. Yanchunis*
Ryan Mcgee*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel.: (813) 223-5505
Fax: (813) 222-4736
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

Jean Sutton Martin*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
2018 Eastwood Road Suite 225

Wilmington, NC 28403
Tel: (813) 559-4908
Fax: (813) 222-4795
jeanmartin@forthepeople.com

Lynda J. Grant
THE GRANT LAW FIRM, PLLC
521 Fifth Avenue, 17th Floor
New York, NY 10175
Tel: (212) 292-4441
Fax: (212) 292-4442
lgrant@grantfirm.com

Ralph N. Sianni
ANDERSON SLEATER SIANNI, LLC
2 Mill Road
Suite 202
Wilmington, DE 19806
Tel: (302) 510-8528
Fax: (302) 595-9321
rsianni@andersensleater.com

Kevin H. Sharp
SANFORD HEISLER SHARP, LLP
611 Commerce Street
Suite 3100
Nashville, TN 37203
Tel: (615) 434-7000
Fax: (615) 434-7020
ksharp@sanfordheisler.com

Counsel for Plaintiffs and the Class

* *pro hac vice* application granted, pending or forthcoming

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document has been furnished to the following individuals via the Court's Electronic Filing System on August 9, 2019:

Gregory T. Parks
Ezra Church
Kristin M. Hadgis
MORGAN, LEWIS
& BOCKIUS LLP
1701 Market Street
Philadelphia, PA 19103
T: (615) 742-4200
F: (615) 742-4539
gregory.parks@morganlewis.com
ezra.church@morganlewis.com
kristin.hadgis@morganlewis.com

/s/ Timothy J. Peter
Timothy J. Peter*
FARUQI & FARUQI, LLP