JOHN A. YANCHUNIS
Admitted Pro Hac Vice
jyanchunis@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiffs and the Proposed Class and Subclasses
[LIST OF ADDITIONAL COUNSEL ON SIGNATURE PAGE]

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

JOWHARAH HAMEED-BOLDEN and ALI CONRAD O'BRIEN, On Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. FOREVER 21 RETAIL, INC., and FOREVER 21, INC. Defendants.	Case No.: 2:18-cv-03019 **FIRST AMENDED CLASS ACTION COMPLAINT FOR:** **(1) California's Unfair Competition Law ("UCL") § 17200 – Unlawful Business Practice;** **(2) UCL § 17200 – Unfair Business Practice** **(3) Deceit by Concealment - Cal. Civil Code §§ 1709, 1710** **(4) Negligence** **(5) Breach of Implied Contract** **(6) Declaratory Judgment**

(7) Violation of California's Customer Records Act – Inadequate Security- Cal. Civ. Code § 1798.81.5

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

Plaintiffs Jowharah Hameed-Bolden and Ali Conrad O'Brien ("Plaintiffs"), on behalf of themselves and all others similarly situated, file this Class Action Complaint against Defendants Forever 21 Retail, Inc. and Forever 21, Inc. (collectively, "Forever 21"), and based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, allege as follows:

SUMMARY OF THE CASE

1. Plaintiffs bring this class action case against Defendants for their failures to secure and safeguard customers' payment card data ("PCD") and other personally identifiable information ("PII") which Forever 21 collected at the time Plaintiffs made purchases at Forever 21 stores, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and Class members that their PCD and PII (hereinafter, collectively, "Customer Data") had been compromised and stolen.

2. Forever 21 is a fashion retailer of women's, men's and kids clothing and accessories.

3. In the last few years, retailers such as Target, Saks Fifth Avenue, Home Depot, Kmart, Neiman Marcus, and Brooks Brothers have experienced stream of attacks on their data security. Implementing measures to prevent those attacks, as well as quickly identifying them is a normal, expected part of the business – except in Forever 21's case. Inexplicably turning a blind eye to this key aspect of its business, Forever 21 did not just

ignore security weaknesses, it failed to set up the systems necessary to even detect them.

4. In November 2017, Forever 21 acknowledged that a third party had "suggested" there might have been a breach of its customers' payment card information.[1] Finally on December 28, 2017, Defendants disclosed that their investigation had determined that hackers had been able to gain access to Forever 21's data systems and install malware to harvest Customer Data for seven months, from April 3 to November 18, 2017 (the "Data Breach").

5. This private Customer Data was compromised due to Forever 21's acts and omissions and their failure to properly protect the Customer Data.

6. Forever 21's sheer recklessness with respect to data security led to predictable results. While the company implemented encryption technology in 2015, the investigation into the Data Breach uncovered that encryption had not been turned on in some of Forever 21's point of sale ("POS") devices.

7. Defendants have admitted that the encryption being turned off allowed the malware to be installed.

8. Adding insult to injury, "Forever 21 stores have a device that keeps a log of completed payment card transaction authorizations. When encryption was off, payment card data was being stored in this log. In a group of stores that were involved in this incident, malware was installed on the log devices that was capable of finding payment card data from the logs, so if encryption was off on a POS device prior to April 3, 2017 and that data was still present in the log filed at one of these stores, the malware could have found that data."

9. In other words, customers who used their payment cards prior to April 3,

[1] https://www.csoonline.com/article/3245069/security/forever-21-hackers-breached-payment-system-for-7-months-no-encryption-on-pos-devices.html (last visited March 4, 2018).

2017 also possibly had their payment card information compromised.

10. Forever 21 could have prevented this Data Breach. Data breaches at other retail establishments in the last few years have been the result of malware installed on POS systems. While many retailers have responded to recent breaches by adopting technology that helps make transactions more secure, Forever 21 did not.

11. In addition to Forever 21's failure to prevent the Data Breach, Forever 21 failed to detect breach while it was ongoing for seven months, and failed to detect the breach itself, only learning of it from a third party.

12. The Data Breach was the inevitable result of Forever 21's inadequate approach to data security and the protection of the Customer Data that it collected during the course of its business. The deficiencies in Forever 21's data security were so significant that the malware installed by the hackers remained undetected and intact for months.

13. The susceptibility of POS systems to malware is well-known throughout the retail industry. In the last five years, practically every major data breach involving retail stores or fast-food restaurant 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."[2] Unfortunately, Forever 21's decisions to ignore these warnings led to the damage upon which this case is based.

14. Forever 21 has recognized that it "understand[s] the importance that [its] customers place on privacy."[3]

---

[2] Datacap Systems Inc., *Point of sale security: Retail data breaches at a glance*, https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance# (last visited March 14, 2018).

[3] Forever 21 Privacy Policy, *available at* https://www.forever21.com/us/shop/Info/PrivacyPolicy (last visited March 14, 2018).

15. Through their Privacy Policy, Forever 21 also represents that it will **"**take commercially reasonable steps to help protect Personal Information from loss, misuse, unauthorized access" and will "encrypt the transmission of that information."

16. Unfortunately, Forever 21 did not hold true to these promises.

17. Forever 21 disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard Customer Data, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

18. In addition, Forever 21 exacerbated the injuries suffered by Plaintiff and the Class by failing to timely detect the infiltration and by failing to timely notify customers their information had been compromised. If Forever 21 had detected the malware earlier and promptly notified the public of the Data Breach, the resulting losses would have been less significant.

19. As a result of the Forever 21 Data Breach, the Customer Data of the Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members as a direct result of the Forever 21 Data Breach include:

a. unauthorized charges on their debit and credit card accounts;

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 debit or credit card accounts because their account were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Forever 21 Data Breach, including but not limited to foregoing cash back rewards;

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 and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Forever 21 Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit card and personal information 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. money paid for merchandise purchased at Forever 21 stores during the period of the Data Breach, in that Plaintiffs and Class members would not have shopped at Forever 21 had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' Customer Data or Plaintiffs and Class members would have taken measures to protect their Customer Data had Defendants made such disclosures;

i. damages to and diminution in value of their Customer Data entrusted to Forever 21 for the sole purpose of purchasing merchandise from Forever 21; and

j. the loss of Plaintiff and Class members' privacy.

20. The injuries to Plaintiffs and Class members were directly and proximately caused by Forever 21's failure to implement or maintain adequate data security measures for Customer Data.

21. Further, Plaintiffs retain a significant interest in ensuring that their Customer Data, which, while stolen, remains in the possession of Defendants is protected from further breaches, and seeks to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose Customer Data was stolen as a result of the Forever 21 Data Breach.

22. Plaintiffs, on behalf of themselves and similarly situated consumers, seek to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the data breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants.

24. This Court has personal jurisdiction over Defendants because Defendant Forever 21 Retail, Inc. is incorporated in California and both Defendants have their headquarters in this District. This Court has personal jurisdiction over Defendants

because Defendants conduct substantial business in the District and because Defendants committed the acts and omissions complained of in the District.

25. Venue is proper under 28 U.S.C. § 1391(c) because Defendants' principal place of business is in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Forever 21's management and IT personnel that led to the Data Breach.

PARTIES

A. Plaintiffs

26. Plaintiff Jowharah Hameed-Bolden is, and for all relevant times has been, a resident and citizen of Sacramento, California.

27. Plaintiff Ali Conrad O'Brien is, and for all relevant times has been, a resident and citizen of Nassau County, New York.

B. Defendants

28. Forever 21 Retail, Inc. is a California corporation with its principal place of business and headquarters located at 3880 N. Mission Road, Room 3030, Los Angeles, California 90031.

29. Forever 21, Inc. is a Delaware corporation registered with the California Secretary of State, with its principal place of business and headquarters located at 3880 N. Mission Road, Room 3030, Los Angeles, California 90031.

FACTUAL BACKGROUND

A. Plaintiffs' Transactions

30. Plaintiff Jowharah Hameed-Bolden made multiple in-store purchases at Forever 21 stores for her children's back-to-school shopping in July and August of 2017. For these purchases, she used her credit union debit card, which she uses only for specific purposes because she has been focusing on building a good credit record. In September

2017, she noticed fraudulent charges on her credit union account. The fraudulent activity caused her account to go into overdraft. As a result, she incurred hundreds of dollars in late fees on other accounts because the fraudulent debits left her without enough money in her account to pay her bills. Additionally, she incurred overdraft fees on her account for the automatic bill-pay attempts made when her account was overdrawn. While her credit union ultimately reimbursed the fraudulent charges, after 6 weeks, the credit union has refused to reverse the overdraft fees she incurred. Due to fraudulent activity on the card, Ms. Hameed-Bolden's credit union issued her a new debit card.

31. Plaintiff Ali Conrad O'Brien made multiple in-store purchases at Forever 21 stores in Nassau and Suffolk counties in New York between April 2017 and October 2017 using her CitiBank Mastercard debit card. She also has an online account with Forever 21 in which her CitiBank Mastercard debit card information is stored. In December 2017, Ms. Conrad O'Brien received an email from Forever 21 thanking her for a recent purchase, which she did not make. Upon investigation, she discovered that someone has used her CitiBank Mastercard debit card to charge $200, for $80 in merchandise and a $120 gift card. Ms. O'Brien spent considerable time working with CitiBank to have the charges reversed.

32. The compromise of Plaintiffs' payment cards occurred even though they had physical possession of their cards at all times. Plaintiffs were required to expend time communicating with the card issuer attempting to resolve the issues caused by the theft of their identities. During the period of time they were awaiting a replacement card, Plaintiffs had to use alternative sources of funds to make purchases.

33. Plaintiffs suffered actual injury from having their Customer Data compromised and stolen in and as a result of the Forever 21 Data Breach.

34. Plaintiffs would not have used their payment cards to make purchases at Forever 21 had Defendants told them that Forever 21 lacked adequate computer systems

and data security practices to safeguard customers' Customer Data from theft. Indeed, Plaintiffs would not have shopped at Forever 21 at all during the period of the Data Breach and, thus, they suffered actual injury and damages in paying money to for the purchase of merchandise from Forever 21 that they would not have paid had Forever 21 made such disclosure.

35. Plaintiffs also suffered actual injury in the form of damages to and diminution in the value of their Customer Data— a form of intangible property that Plaintiffs entrusted to Forever 21 as a form of payment for merchandise and that was compromised in and as a result of the Data Breach.

36. Additionally, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their Customer Data being placed in the hands of criminals who have already misused such information, as evidenced by the compromise of Plaintiffs' payment cards.

37. Moreover, Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of Forever 21, is protected and safeguarded from future breaches.

B. Forever 21 Collects and Stores PII for its Own Financial Gain

38. Founded in 1984, Forever 21 operates more than 800 stores in 57 countries, including the United States.

39. In 2017, Forever 21 earned more than $4 billion in sales.

40. With its growing profitability, Forever 21 heavily invested in opening 40 new retail locations in the U.S. in 2017.[4]

41. Despite Forever 21's substantial investments made to expand its retail presence, Forever 21 failed to make meaningful improvements to the security of its POS

[4] https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=4220077 (last visited March 24, 2018).

systems and administrative network, placing the purchasing information of its customers at risk.

42. A significant portion of sales at Forever 21 brick-and-mortar stores, as well as their online store, are made using credit or debit cards. When customers pay using credit or debit cards, Forever 21 collects Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Forever 21 stores the Customer Data in its POS system and transmits this information to a third party for processing and completion of the payment.

43. A significant portion of sales at Forever 21 are made using credit or debit cards. When customers pay using credit or debit cards, Forever 21 collects Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. Forever 21 stores the Customer Data in its POS system and transmits this information to a third party for processing and completion of the payment.

44. At all relevant times, Forever 21 was well-aware, or reasonably should have been aware, that the Customer Data collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

45. It is well known and the subject of many media reports that Customer Data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches by other retailers, Forever 21 maintained an insufficient and inadequate system to protect the Customer Data of Plaintiffs and Class members.

46. Customer Data is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, and other personal information on a number of underground Internet websites. Customer Data 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.

47. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[5]

48. At all relevant times, Forever 21 knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

49. Forever 21 was, or should have been, fully aware of the significant volume of daily credit and debit card transactions at Forever 21 retail locations, and thus, the significant number of individuals who would be harmed by a breach of Forever 21's systems.

50. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of Customer Data in the hands of other third parties, such as retailers, Forever 21's approach to maintaining the privacy and security of the Customer Data of Plaintiffs and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

[5] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 10, 2017).

C. Forever 21 Had Notice of Data Breaches Involving Malware on POS Systems

51. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[6] 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.[7] 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.[8]

52. Most of the massive data breaches occurring within the last several years involved malware placed on POS systems used by retail merchants. A POS system is an on-site device, much like an electronic cash register, which manages transactions from consumer purchases, both by cash and card. 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 networks before reaching the retailer's payment processor." [9] The payment processor then passes on the payment information to the financial institution that issued the card and takes the other steps needed to complete the transaction.[10]

---

[6] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), http://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208 (last visited July 17, 2017).

[7] *Id*.

[8] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), available at: https://origin-www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf (last visited July 17, 2017).

[9] *Id*. at 6.

[10] Salva Gomzin, *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions*, 8 (Wiley 2014), *available at:* http://1.droppdf.com/files/IS0md/wiley-hacking-point-of-sale-payment-application-secrets-threats-and-solutions-2014.pdf (last visited July 18, 2017).

53. 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.[11] The stored information includes "Track 1" and "Track 2" data from the magnetic strip on the payment card, such as the cardholder's first and last name, the expiration date of the card, and the CVV (three number security code on the card).[12] This information is unencrypted on the card and, at least briefly, will be unencrypted in the POS terminal's temporary memory as it processes the data. [13]

54. In ordered to directly access a POS device, hackers generally follow four steps: infiltration, propagation, exfiltration and aggregation.[14] In the infiltration phase, an "attacker gains access to the target environment"[15] allowing the hackers to move through a business's computer network, find an entry point into the area that handles consumer payments, and directly access the physical POS machines at in-store locations.[16] Once inside the system the attacker then infects the POS systems with malware, which "collects the desired information . . . and then exfiltrates the data to another system" called the "aggregation point."[17]

55. A 2016 report by Verizon confirmed "[t]he vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to

---

[11] *Id*. at 39.
[12] *Id*. at 43-50.
[13] Symantec, *supra* note 8, at 5.
[14] *Point of Sale Systems and Security: Executive Summary*, SANS Institute, 4 (Oct. 2014), available at: https://www.sans.org/reading-room/whitepapers/analyst/point-salesystems-security-executive-summary-35622 (last visited July 18, 2017).
[15] *Id*.
[16] Symantec, *supra* note 8, at 6.
[17] *Id*.

capture payment card data."[18] 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.[19]

56. 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."[20] Since 2014, malware installed on POS systems has been responsible for nearly every major data breach of a retail outlet or restaurant.[21] In 2015, intrusions into POS systems accounted for 64% of all breaches where intruders successfully stole data.[22] For example, in 2013, hackers infiltrated Target, Inc.'s POS system, stealing information from an estimated 40 million payment cards in the United States.[23] In 2014, over 7,500 self-checkout POS terminals at Home Depots throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[24]

57. Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, Forever 21 was well aware or should have been aware of the need to safeguard its POS systems.

---

[18] *Id*.
[19] *2016 Data Breach Investigations Report*, Verizon, at 4 (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Retail-DataSecurity_en_xg.pdf. (last visited July 18, 2017).
[20] Symantec, *supra* note 8, at 3.
[21] Verizon, *supra* note 19, at 1.
[22] *Id*. at 3.
[23] Brian Krebs, *Fast Food Chain Arby's Acknowledges Breach*, KrebsOnSecurity (Feb. 17, 2017), https://krebsonsecurity.com/2017/02/fast-food-chain-arbysacknowledges-breach/ (last visited July 18, 2017).
[24] Brett Hawkins, *Case Study: The Home Depot Data Breach*, 7 (SANS Institute, Jan. 2015), available at: https://www.sans.org/reading-room/whitepapers/casestudies/casestudy-home-depot-data-breach-36367 (last visited July 18, 2017).

D. The 2017 Forever 21 Data Breach

58. Finally, on December 28, 2017, Defendant disclosed that its investigation had determined that hackers had been able to gain access to Forever 21's data systems and install malware to harvest Customer Data. The malware allowed the thieves to download and steal copies of Customer Data for seven months, from April 3 to November 18, 2017 (the "Data Breach").

59. Forever 21 implemented the use of encryption technology in 2015. Encryption is usually used by the store to protect its payment processing system. However, the investigation into the Data Breach determined that the encryption on some POS devices "was not always on," opening up the POS terminals to malware.[25]

60. Causing additional trouble for consumers, "Forever 21 stores have a device that keeps a log of completed payment card transaction authorizations. When encryption was off, payment card data was being stored in this log. In a group of stores that were involved in this incident, malware was installed on the log devices that was capable of finding payment card data from the logs, so if encryption was off on a POS device prior to April 3, 2017 and that data was still present in the log filed at one of these stores, the malware could have found that data." Meaning, customers who used their payment cards prior to April 3, 2017 also possibly had their payment card information compromised.

61. Forever 21 has stated that payment card transactions through its online store were not impacted by the Data Breach.

62. Forever 21 has not disclosed how many customers had their Customer Data compromised and stolen.

63. The Data Breach resulted from Forever 21's acts and omissions and failure

[25] https://www.csoonline.com/article/3245069/security/forever-21-hackers-breached-payment-system-for-7-months-no-encryption-on-pos-devices.html (last visited March 24, 2018).

to properly protect the Customer Data, despite being aware of recent data breaches impacting other national retailers.

64. The Data Breach occurred because Forever 21 failed to implement adequate data security measures to protect its POS networks from the potential danger of a data breach and failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Customer Data compromised in the Data Breach.

65. While many merchants have responded to recent breaches by adopting technology and security practices that help make transactions and stored data more secure, Forever 21 has not done so.

66. The Data Breach was caused and enabled by Forever 21's knowing violation of their obligations to abide by best practices and industry standards in protecting Customer Data.

67. In addition to Forever 21's failure to prevent the Data Breach, Forever 21 also failed to detect the breach for seven months.

68. Intruders, therefore, had months to collect Customer Data unabated. During this time, Forever 21 failed to recognize its systems had been breached and that intruders were stealing data on millions of payment cards. Timely action by Forever 21 likely would have significantly reduced the consequences of the breach. Instead, Forever 21 took more than half a year to realize its systems had been breached, and thus contributed to the scale of the Breach and the resulting damages.

E. Forever 21 Turns a Blind Eye to Security, Even After Repeated Intrusions

69. In 2008, Forever 21 announced that hackers had accessed payment data on nine different dates between November 2003 and August 2007. [26] Defendant came to learn of this breach only when the U.S. Secret Service gave the company a disk containing almost

[26] Csoonline, *supra* note 25.

100,000 compromised payment card numbers of Forever 21 customers.

70. In response to learning about that breach, five years after it began, Forever 21 sent notification letters to affected customers. *Id.* Forever 21 also stated that it had implemented additional security measures but was evasive about what those were. *Id*.

71. In 2015, Forever 21 apparently implemented encryption technology on its POS systems. But for some reason, the encryption technology was "not always on" in its stores.

72. Forever 21 has stated that it is working to ensure banks that issue the payment cards compromised in the breach are made aware of the incident, but to date, Forever 21 has not sent notification letters to affected customers as it did in 2008.

F. Forever 21 Failed to Comply with Industry Standards

73. Despite the vulnerabilities of POS systems, available security measures and reasonable businesses practices would have significantly reduced or eliminated the likelihood that hackers could successfully infiltrate business' POS systems. One report indicated that over 90% of the data breaches occurring in 2014 were preventable.[27]

74. 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 Forever 21's 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 the multiple breaches of the POS systems at other retailers, Forever 21failed to adhere to these guidelines and failed to take reasonable and sufficient protective measures to prevent the Data Breach.

75. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, more than two years ago, Symantec

[27] Verizon, *supra* note 5, at 1.

recommended "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.[28] Moreover, Symantec emphasized the importance of adopting EMV chip technology. Likewise, Datacap Systems, a developer of POS systems, recommended similar preventative measures.[29]

76. 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.

77. 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.[30]

78. 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."[31] PCI DSS sets the minimum level of what must be done, not the maximum.

79. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, impose the following mandates on Forever 21:[32]

---

[28] Symantec, *supra* note 8, at 6.
[29] *See* Datacap Systems, *supra* note 2.
[30] *Payment Card Industry Data Security Standard* v3.2, at 5 (April 2016) available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited March 24, 2018).
[31] *Id*.
[32] *Id*.

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

80. Among other things, PCI DSS required Forever 21 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.

81. PCI DSS also required Forever 21to 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.[33]

82. Despite Forever 21's awareness of its data security obligations, Forever 21's treatment of PCD and PII entrusted to it by its customers fell far short of satisfying Forever 21's legal duties and obligations and included violations of the PCI DSS. Forever 21 failed to ensure that access to its 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.

[33] *Id*. at 38 (PCI DSS 3.2.1 and 3.2.2).

G. Forever 21 Failed to Upgrade its Payment Systems to Use More Secure Technology

83. The payment card industry also sets rules requiring all businesses to upgrade to new card readers that accept EMV chips. Data Security advisors, like Symantec and DataCap Systems, have also strongly encouraged the use of POS terminals capable of accepting payment from EMV chips.

84. EMV chip technology uses embedded computer chips instead of magnetic stripes to store PCD. The magnetic stripe on the back of a debit or credit card contains a code that is recovered by sliding the card through a magnetic stripe reader. The code never changes. Unlike magnetic stripe technology, in which the card information never changes, EMV technology creates a unique transaction code every time the chip is used. Such technology increases payment card security because the unique transaction code cannot be used again, making it more difficult for criminals to use stolen EMV chip card information.

85. The payment card industry, including Visa, MasterCard, and American Express, set a deadline of October 1, 2015 for businesses to transition their POS systems from magnetic stripe readers to readers using EMV chip technology.

86. Upon information and belief, Forever 21 has not implemented EMV technology at its retail stores.

H. Forever 21 Failed to Comply With FTC Requirements

87. 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 business 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.[34]

88. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[35] 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.

89. 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 activity on the network; and verify that third-party service providers have implemented reasonable security measures.[36]

90. 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

---

[34] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 10, 2017).

[35] 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 April 10, 2017).

[36] FTC, *Start With Security*, *supra* note 34.

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.

91. Forever 21's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

92. In this case, Forever 21was at all times fully aware of its obligation to protect the financial data of Forever 21's customers because of its participation in payment card processing networks. Forever 21 was also aware of the significant repercussions if it failed to do so because Forever 21 collected payment card data from tens of thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and Class members.

93. Despite understanding the consequences of inadequate data security, Forever 21 failed to comply with PCI DSS requirements and failed to take additional protective measures beyond those required by PCI DSS.

94. Despite understanding the consequences of inadequate data security, Forever 21 operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect its data network.

I. The Data Breach Caused Harm and Will Result in Additional Fraud

95. Without detailed disclosure of the nature and scope of the Data Breach, consumers, including Plaintiffs and Class members, have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

96. The ramifications of Forever 21's failure to keep Plaintiffs' and Class members' data secure are severe.

97. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[37] 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."[38]

98. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[39]

99. Identity thieves can use personal information, such as that of Plaintiffs and Class members which Forever 21 failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

100. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[40]

---

[37] 17 C.F.R § 248.201 (2013).
[38] *Id.*
[39] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).
[40] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).

101. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[41]

102. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[42]

103. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

---

[41] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited March 24, 2018).

[42] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited March 24, 2018).

J. Plaintiffs and Class Members Suffered Damages

104. The Customer Data of Plaintiffs and Class members is private and sensitive in nature and was left inadequately protected by Forever 21. Forever 21 did not obtain Plaintiff's and Class members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

105. The Data Breach was a direct and proximate result of Forever 21's failure to properly safeguard and protect Plaintiffs' and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Forever 21's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

106. Forever 21 had the resources to prevent a breach, having dramatically increased its overall annual sales in the last few years. Forever 21 made significant expenditures to open new retail locations in 2017, but neglected to adequately invest in data security, despite the growing number of POS intrusions and several years of well-publicized data breaches.

107. Had Forever 21 remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Forever 21 would have prevented intrusion into its POS systems and, ultimately, the theft of its customers' confidential payment card information.

108. As a direct and proximate result of Forever 21's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated

to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

109. Forever 21's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;
b. unauthorized charges on their debit and credit card accounts;
c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet card black market;
d. the untimely and inadequate notification of the Data Breach;
e. the improper disclosure of their Customer Data;
f. loss of privacy;
g. the monetary amount of purchases at Forever 21 during the period of the Data Breach in that Plaintiffs and Class members would not have shopped at Forever 21, or at least would not have used their payment

cards for purchases, had Forever 21 disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Forever 21 provided timely and accurate notice of the Data Breach;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

i. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. loss of use of and access to their account funds and costs associated with the 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 adverse credit notations; and,

l. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

110. Forever 21 has not offered customers any credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage Forever 21 has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Forever 21's actions have created for Plaintiff and Class members, is ascertainable and is a determination appropriate for the trier of fact. Forever 21 has also not offered to cover any of the damages sustained by Plaintiff or Class members.

111. While the Customer Data of Plaintiffs and members of the Class has been stolen, Forever 21 continues to hold Customer Data of consumers, including Plaintiffs and Class members. Particularly because Forever 21 and has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and members of the Class have an undeniable interest in insuring that their Customer Data is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CHOICE OF LAW

112. California, which seeks to protect the rights and interests of California and other U.S. residents against a company doing business in California, has a greater interest in the claims of Plaintiffs and the Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

113. The principal place of business of Forever 21, located at 3880 N. Mission Road, Los Angeles, California, is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security, and where: a) major policy, b) advertising, c) distribution, d) accounts receivable departments and e) financial and legal decisions originate.

114. Forever 21's corporate point-of-sale system and IT personnel operate out of and are located at Forever 21's headquarters in California. PCI-DSS assessments and other duties related to POS systems and data security occur at Forever 21's California headquarters.

115. Furthermore, Forever 21's response to, and corporate decisions surrounding such response to, the Data Breach were made from and in California.

116. Forever 21's breach of its duty to customers, and Plaintiffs, emanated from California.

117. Moreover, because Defendants are headquartered in California and their key decisions and operations emanate from California, California law can and should apply to claims relating to the Forever 21 Data Breaches, even those made by persons who reside outside of California. In fact, California law should apply to all Plaintiffs' claims, as Defendants' decisions and substandard acts happened in California, and upon information and belief, the Plaintiffs' PII was collected, stored on, and routed through California, and United States-based servers. For the sake of fairness and efficiency, California law should apply to these claims.

118. Application of California law to a nationwide Class with respect to Plaintiffs' and the Class members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs and the nationwide Class.

119. Further, under California's choice of law principles, which are applicable to this action, the common law of California will apply to the common law claims of all Class members.

CLASS ACTION ALLEGATIONS

120. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs bring this lawsuit on behalf of themselves and as a class action on behalf of the following Class:

> All persons residing in the United States who made a credit or debit card purchase at any affected Forever 21 location from April 3, 2017 through November 18, 2017.

121. Plaintiff Jowharah Hameed-Bolden brings this lawsuit on behalf of herself and as a class action on behalf of the following California state subclass:

> All persons residing in California who made a credit or debit card purchase at any affected Forever 21 location from April 3, 2017 through November 18, 2017.

122. Excluded from the Class and California subclass are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest; Defendants' officers, agents, and employees; and all persons who make a timely election to be excluded from the Class. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

123. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. Plaintiffs reasonably believe that Class members number hundreds of millions of people or more in the aggregate and well over 1,000 in the smallest of the classes. The names and addresses of Class members are identifiable through documents maintained by Defendants.

124. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

a. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Class members' PII was accessed, compromised, or stolen in the Data Breach;

d. Whether Defendants failed to timely notify the public of those Breaches;

e. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

f. Whether Defendants' conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80 *et seq.*;

g. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*,

h. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

i. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

125. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the members of their respective classes. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

126. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiffs and the other class members were injured through the substantially uniform misconduct by Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and

all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

127. **Adequacy of Representation:** Plaintiffs are adequate representatives of the classes because their interests do not conflict with the interests of the other Class 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 members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

128. **Superiority:** 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 matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase 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 single adjudication, economies of scale, and comprehensive supervision by a single court.

129. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

130. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Class members' PII was accessed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendants knew about the Data Breach before they were announced to the public and whether Defendants failed to timely notify the public of the Breach;

c. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

d. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class members' Customer Data;

e. Whether Defendants concealed crucial information about their inadequate data security measures from Plaintiffs and the Class;

f. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

g. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

h. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' Customer Data secure and prevent the loss or misuse of that information;

i. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class members' Customer Data in violation of Cal. Civ. Code § 1798.81.5, and Section 5 of the FTC Act;

j. Whether Defendants failed to provide timely notice of the Data Breach, to Plaintiffs and Class members in violation of California Civil Code § 1798.82;

k. Whether Defendants owed a duty to Plaintiffs and the Class to safeguard their Customer Data and to implement adequate data security measures;

l. Whether Defendants breached that duty;

m. Whether an implied contract existed between Defendants and Plaintiffs and the Class members and the terms of that implied contract; and,

n. Whether Defendants breached the implied contract.

First Claim for Relief
Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq*.)

131. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 130 as though fully stated herein.

132. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

133. As discussed above, Forever 21's acts, practices, and omissions at issue in this matter, particularly those related to data security, were directed and emanated from its headquarters in Los Angeles, California.

134. By using their payment cards as methods of payment, which Forever 21 accepted, Plaintiff and Class members entrusted Forever 21 with their private Customer Data.

135. Defendants stored the PII and PCD of Plaintiffs and the Class 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 other Class members' Customer Data secure and prevented the loss or misuse of Plaintiffs' and the other Class members' Customer Data. Forever 21 did not disclose to Plaintiffs and of Class members that its data systems were not secure.

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

137. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of its many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class members' Customer Data. Defendants also violated the UCL 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 other Class members of the Data Breach. If Defendants had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages related to the Data Breach.

138. Further, as alleged herein this Complaint, Forever 21 engaged in unlawful business practices in the conduct of business transactions, in violation of the UCL, by and including, it's:

a. failure to maintain adequate computer systems and data security practices to safeguard Customer Data;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Customer Data from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members;

d. continued acceptance of credit and debit card payments and storage of other personal information after Forever 21 knew or should have known of the security vulnerabilities of the POS systems that were exploited in the Data Breach; and

e. continued acceptance of credit and debit card payments and storage of other personal information after Forever 21 knew or should have known of the Data Breach and before it allegedly remediated the Breach.

139. Furthermore, as alleged above, Forever 21's failure to secure consumers' Customer Data violates the FTCA and therefore violates the UCL.

140. Forever 21 knew or should have known that its computer and POS systems and data security practices were inadequate to safeguard the Customer Data of Plaintiffs and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

141. Because Forever 21 accepted credit and debit cards as methods of payment, Plaintiffs and Class members relied upon Forever 21 to advise customers if its POS and data systems were not secure and, thus, Customer Data could be compromised.

142. Plaintiffs and Class members were not afforded by Forever 21 equal or ample opportunity to make any inspection to determine Forever 21's data security or to otherwise ascertain the truthfulness of Defendant's direct and indirect representations regarding data security, including Forever 21's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

143. In deciding to use their payment cards for their purchases at Forever 21, Plaintiffs and Class members relied upon Forever 21's direct and indirect representations regarding data security, including Forever 21's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

144. Had Forever 21 disclosed to Plaintiffs and Class members that its POS and data systems were not secure and, thus, vulnerable to attack, Plaintiffs and Class members would not have used their payment cards at Forever 21, and very well may not have made purchases at all at Forever 21 stores.

145. Plaintiffs and Class members would not have given their PII and PCD to Forever 21 if Forever 21 had disclosed the security issues.

146. As a direct result of their reliance upon Forever 21 to be truthful in its disclosures and non-disclosures regarding the vulnerability of its POS and data systems, Plaintiffs and Class members used their payment cards to make purchases at Forever 21 during the Data Breach period and their Customer Data was compromised causing Plaintiffs and Class members to suffer damages.

147. As a direct result of Forever 21's refusal to disclose that its data systems were not secure, Plaintiffs and Class members:

a. surrendered more in their transactions that they otherwise would have had;

b. entered into transactions costing money or property that they otherwise would not have entered;

c. had the value of their PII diminished; and,

d. had their PII compromised causing losses and damages, and thus were deprived of money and property

148. As a direct and proximate result of Forever 21's violation of the UCL, Plaintiffs and Class members suffered damages including, but not limited to: diminution of their PII, damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Plaintiffs and Class members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. In addition, their PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

149. As a result of Defendants' unlawful business practices, violations of the UCL, Plaintiffs and the members of the Class are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

Second Claim for Relief
Violation of California's Unfair Competition Law ("UCL") –
Unfair Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq*.)

150. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 130 as though fully stated herein.

151. As discussed above, Forever 21's acts, practices, and omissions at issue in this matter, particularly those related to data security, were directed and emanated from its headquarters in Los Angeles, California.

152. By using their payment cards as methods of payment, which Forever 21 accepted, Plaintiffs and Class members entrusted Forever 21 with their private Customer Data.

153. By reason of the conduct alleged herein, Defendants engaged in unfair practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

154. Defendants stored the PII of Plaintiffs and members of their respective Classes 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 other Class members' Customer Data secure and prevented the loss or misuse of Plaintiffs' and the other Class members' Customer Data. Forever 21 did not disclose to Plaintiffs and of Class members that its data systems were not secure.

155. Plaintiffs and Class members were entitled to assume, and did assume, Defendants would take appropriate measures to keep their Customer Data safe. Defendants did not disclose at any time that Plaintiffs' Customer Data was vulnerable to hackers because Defendants' data security measures were inadequate, and Defendants

were the only ones in possession of that material information, which they had a duty to disclose.

156. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of its many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class members' Customer Data. Defendants also violated the UCL 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 other Class members of the Data Breach. If Defendants had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages related to the Data Breach.

157. Further, as alleged herein this Complaint, Forever 21 engaged in unfair business practices in the conduct of business transactions, in violation of the UCL, by and including, it's:

a. failure to maintain adequate computer systems and data security practices to safeguard Customer Data;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Customer Data from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiffs and Class members;

d. continued acceptance of credit and debit card payments and storage of other personal information after Forever 21 knew or should have known of the security vulnerabilities of the POS systems that were exploited in the Data Breach; and

e. continued acceptance of credit and debit card payments and storage of other personal information after Forever 21 knew or should have known of the Data Breach and before it allegedly remediated the Breach.

158. Furthermore, as alleged above, Forever 21's failure to secure consumers' Customer Data violates the FTCA and therefore violates the UCL.

159. Forever 21 knew or should have known that its computer and POS systems and data security practices were inadequate to safeguard the Customer Data of Plaintiffs and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

160. Because Forever 21 accepted credit and debit cards as methods of payment, Plaintiffs and Class members relied upon Forever 21 to advise customers if its POS and data systems were not secure and, thus, Customer Data could be compromised.

161. Plaintiffs and Class members were not afforded by Forever 21 equal or ample opportunity to make any inspection to determine Forever 21's data security or to otherwise ascertain the truthfulness of Defendants' direct and indirect representations regarding data security, including Forever 21's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

162. In deciding to use their payment cards for their purchases at Forever 21, Plaintiffs and Class members relied upon Forever 21's direct and indirect representations regarding data security, including Forever 21's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

163. Had Forever 21 disclosed to Plaintiffs and Class members that its POS and data systems were not secure and, thus, vulnerable to attack, Plaintiffs and Class members would not have used their payment cards at Forever 21, and very well may not have made purchases at all at Forever 21 stores.

164. As a direct result of their reliance upon Forever 21 to be truthful in its disclosures and non-disclosures regarding the vulnerability of its POS and data systems, Plaintiffs and Class members used their payment cards to make purchases at Forever 21

s during the Data Breach period and their Customer Data was compromised causing Plaintiff and Class members to suffer damages.

165. As a direct and proximate result of Forever 21's violation of the UCL, Plaintiffs and Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Plaintiffs and Class members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

166. As a result of Defendants' unfair business practices, violations of the UCL, Plaintiffs and the members of the Class are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

167. **Defendants engaged in unfair business practices under the "balancing test."** The harm caused by Forever 21's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Forever 21's' failure to follow

basic data security protocols cannot be said to have had any utility at all. And, there was no utility, other than perhaps to Defendants themselves, in failure to advise consumers about Forever 21's inadequate data security while accepted payment cards and unreasonably waiting to disclose the Data Breach to its customers. All of these actions and omissions were clearly injurious to Plaintiffs and the Class members, directly causing the harms alleged below.

168. **Defendants engaged in unfair business practices under the "tethering test."** Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendants' acts and omissions, and the injuries caused by them are thus "comparable to or the same as a violation of the law …" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

169. **Defendants engaged in unfair business practices under the "FTC test."** The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects perhaps millions of Class members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Class members' Customer Data to third parties without their consent, diminution in value of their Customer Data, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other

expenses relating to identity theft losses or protective measures. This harm continues given the fact that Class members' Customer Data remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

170. Defendants' actions and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of personal information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

171. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Forever 21, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of Forever 21's duty in this regard.

172. Forever 21 violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, as described in detail herein. Forever 21's conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored, and the foreseeable consequences of a data breach at a retail chain as large as Forever 21, including, specifically, the immense damages that would result to Plaintiffs and Class members.

173. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

174. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

175. **Defendants engaged in unfair business practices by violating Section 1798.82 of the California Customer Records Act ("CRA")**. Section 1798.82 of the CRA requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay …"

176. The statute further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is

reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

177. The security breach notification required under the CRA shall be written in plain language and shall include, at a minimum, the following information:

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred.

d. The date of the notice;

e. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

f. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

g. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

178. The Data Breach described herein this Complaint constitutes a "breach of the security system" of Defendants.

179. As alleged above, Defendants unreasonably delayed informing members of the California subclass about the Data Breach, affecting the confidential and non-public

Customer Data of Plaintiff Hameed-Bolden and the members of the California subclass, after Forever 21 knew the Data Breach had occurred.

180. Defendants failed to disclose to Plaintiff Hameed-Bolden and the members of 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, Customer Data when Defendants knew or reasonably believed such information had been compromised.

181. Forever 21's ongoing business interests gave Defendants incentive to conceal the Data Breach from the public to ensure continued revenue.

182. Upon information and belief, no law enforcement agency instructed Defendants that notification to Plaintiff Hameed-Bolden and the members of the California subclass would impede its investigation.

183. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiff Hameed-Bolden and the members of the California subclass were deprived of prompt notice of the Data 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 Forever 21 stores, securing identity theft protection, or requesting a credit freeze. These measures would have prevented some or all of the damages suffered by Plaintiff Hameed-Bolden and the members of the California subclass because their stolen information would not have any value to identity thieves.

184. As a result of Defendants' unlawful practices in violation of the UCL, Plaintiffs and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Plaintiffs and Class members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result

of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

185. As a result of Defendants' unfair business practices, violations of the UCL, Plaintiffs and Class members are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

Third Claim for Relief

Deceit by Concealment — Cal. Civil Code §§ 1709, 1710

186. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 130 as though fully stated herein.

187. As alleged above, Forever 21 knew its data security measures were grossly inadequate by, at the absolute latest, 2008.

188. In response to this knowledge and a previous breach, Defendants chose to do nothing to protect Plaintiffs and the Class or warn them about the security problems and breaches.

189. Defendants had an obligation to disclose to Class members that Forever 21's POS systems were an easy target for hackers and Defendants were not implementing measures to protect them.

190. Defendants did not do these things. Instead, Defendants willfully deceived Plaintiffs and the Class by concealing the true facts concerning their data security, which Defendants were obligated to, and had a duty to, disclose.

191. Defendant's duty to disclose the inadequacy of its data security measures also arose from the special relationship between Defendants and Plaintiffs and the Class. First, Plaintiffs and the Class purchased merchandise from Forever 21 and in exchange made payment to Defendants. However, an additional relationship was formed when Forever 21 offered Plaintiffs and the Class the ability to use payment cards as an approved form of payment and in exchange undertook a duty to protect the personal data attached to those payment cards.

192. Plaintiffs and the Class accepted Forever 21's offer to use payment cards with the understanding that Defendants would take appropriate measures to protect their Customer Data and would inform Plaintiffs and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But, Defendants did not. Defendants not only knew their data security was inadequate, they also knew they didn't even have the tools to detect and document intrusions or exfiltration of Customer Data.

193. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Defendants' failure to disclose to Plaintiffs and the Class the knowledge that their systems and technologies for processing and securing the Customer Data had numerous security vulnerabilities.

194. Defendants are morally culpable given their inadequate approach to data security, the deficiencies of which were so significant that the malware installed by the hackers remained undetected and intact for months, and their refusal to notify their customers of their security vulnerabilities while continuing to accept payment cards as methods of payment.

195. Defendants' concealment of their knowledge and failure to adequately protect the Customer Data of Plaintiffs and the Class implicates the consumer data protection concerns expressed in California statutes, such as the CRA and CLRA.

196. Had Defendants disclosed the true facts about their dangerously poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, and Defendants did not.

197. Independent of any representations made by Defendants, Plaintiffs and the Class justifiably relied on Defendants to provide at least minimally adequate security measures and justifiably relied on Defendants to disclose facts undermining that reliance when accepted payment cards as methods of payment.

198. In spite of Defendants' knowledge, at least as early as 2008, that its data security had multiple vulnerabilities, Forever 21 continued accepting payment cards as methods of payment while failing to warn its customers that they did not have adequate protection measures.

199. Because Forever 21 accepted credit and debit cards as methods of payment, Plaintiffs and Class members relied upon Forever 21 to advise customers if its POS and data systems were not secure and, thus, Customer Data could be compromised.

200. Plaintiffs and Class members were not afforded by Forever 21 equal or ample opportunity to make any inspection to determine Forever 21's data security or to otherwise ascertain the truthfulness of Defendant's direct and indirect representations regarding data security, including Forever 21's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

201. In deciding to use their payment cards for their purchases at Forever 21, Plaintiffs and Class members relied upon Forever 21's direct and indirect representations

regarding data security, including Forever 21's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

202. Had Forever 21 disclosed to Plaintiffs and Class members that its POS and data systems were not secure and, thus, vulnerable to attack, Plaintiffs and Class members would not have used their payment cards at Forever 21, and very well may not have made purchases at all at Forever 21 stores.

203. Plaintiffs and Class members would not have given their PII and PCD to Forever 21 if Forever 21 had disclosed the security issues

204. Had Defendants disclosed the true facts about their dangerously poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, and Defendants did not.

205. Alternatively, given the gaping security holes in Defendants' data security practices and Defendants' refusal to take measures to even detect those holes, much less fix them, Defendants simply should have stopped taking payment cards as a form of payment.

206. Rather than disclosing to Plaintiffs and the Class that its systems were unsafe, and Customer Data was at risk to theft on a grand scale, Forever 21 continued on and willfully suppressed any information relating to the inadequacy of its security.

207. Defendants' actions constitute "deceit" under Cal. Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

208. As a result of this deceit by Defendants, they are liable under Cal. Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

209. As a result of this deceit by Defendants, the Customer Data of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Customer Data was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their Customer Data in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for overdraft charges, late fees, other bank charges, procuring credit freeze and protection services, and other expenses relating to identity theft losses or protective measures.

210. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants under Civil Code § 3294(a).

Fourth Claim for Relief
Negligence

211. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 130 as though fully stated herein.

212. Upon accepting and storing the Customer Data of Plaintiffs and Class members in its computer systems and on its networks, Forever 21 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. Forever 21 knew that the Customer Data was private and confidential and should be protected as private and confidential.

213. Forever 21 owed a duty of care not to subject Plaintiffs and Class members, along with their Customer Data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

214. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their Customer Data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure the Customer Data of Plaintiffs' and the Class was adequately secured and protected, including turning on the encryption technology Forever 21 had implemented. Defendants further had a duty to implement processes that would detect a breach of their data system in a timely manner.

215. Defendants knew that the Customer Data of Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if the Customer Data of Plaintiffs and the Class was wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class were not told about the disclosure in a timely manner.

216. By being entrusted by Plaintiffs and the Class to safeguard their Customer Data, Defendants had a special relationship with Plaintiffs and the Class. First, Plaintiffs and the Class purchased merchandise from Forever 21 and in exchange made payment to Defendants. However, an additional relationship was formed when Forever 21 offered Plaintiffs and the Class the ability to use payment cards as an approved form of payment and in exchange undertook a duty to protect the personal data attached to those payment cards. This special relationship between Defendants and Plaintiffs and the Class further solidifies the duty owed by Defendants to protect the Customer Data of Plaintiffs and the Class.

217. Plaintiffs and the Class accepted Forever 21's offer to use payment cards with the understanding that Defendants would take appropriate measures to protect their Customer Data and would inform Plaintiffs and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But, Defendants

did not. Defendants not only knew their data security was inadequate, they also knew they didn't even have the tools to detect and document intrusions or exfiltration of Customer Data.

218. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other class members' Customer Data. Defendants knew their systems and technologies for processing and securing the Customer Data of Plaintiffs and the Class had numerous security vulnerabilities.

219. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Customer Data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite previous intrusions, and allowing unauthorized access to Plaintiffs' and the other Class members' Customer Data.

220. Defendants also breached their duty to timely disclose that Plaintiffs' and the other Class members' Customer Data had been, or was reasonably believed to have been, stolen or compromised.

221. Defendants' failure to comply with industry and federal regulations further evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Customer Data.

222. Defendants' breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Defendants to acknowledge and correct serious and ongoing data security problems.

223. Defendants are morally culpable given their inadequate approach to data security, the deficiencies of which were so significant that the malware installed by the hackers remained undetected and intact for months, and their refusal to notify their

customers of their security vulnerabilities while continuing to accept payment cards as methods of payment.

224. Defendants' concealment of their knowledge and failure to adequately protect the Customer Data of Plaintiffs and the Class implicates the consumer data protection concerns expressed in California statutes, such as the CRA and CLRA.

225. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and the Class, their Customer Data would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the Customer Data of Plaintiffs and the Class and all resulting damages.

226. As a result of this misconduct by Defendants, the Customer Data of Plaintiffs and the Class was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Customer Data was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their Customer Data in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

227. Defendants' misconduct as alleged herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants under Civil Code § 3294(a).

228. Having substantiated a claim of ordinary negligence, Plaintiffs are entitled to a presumption of *negligence per se* based upon Defendants' violation of the FTC Act. Alternatively, Defendants' violation of the FTC Act is evidence of their negligence.

229. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Forever 21, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of Forever 21's duty in this regard.

230. Forever 21 violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, as described in detail herein. Forever 21's conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored, and the foreseeable consequences of a data breach at a retail chain as large as Forever 21, including, specifically, the immense damages that would result to Plaintiffs and Class members.

231. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

232. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

233. As a direct and proximate result of Forever 21's violation of Section 5 of the FTC Act, Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies,

contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

Fifth Claim for Relief
Breach of Implied Contract

234. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 130 as though fully stated herein.

235. Forever 21 solicited and invited Plaintiffs and Class members to make purchases using their credit or debit cards. Plaintiffs and Class members accepted Forever 21's offers and used their credit or debit cards to make purchases at Forever 21 stores during the period of the Data Breach.

236. When Plaintiffs and Class members purchased and paid for merchandise at Forever 21 stores using payment cards, they provided their Customer Data, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiffs and Class members entered into implied contracts with Forever 21 pursuant to which Forever 21 agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised.

237. Each purchase at Forever 21 made by Plaintiffs and Class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with Forever 21 under which Forever 21 agreed to safeguard and protect the Customer Data of Plaintiff and Class members, including all information contained in the magnetic stripe of Plaintiffs' and Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

238. Plaintiffs and Class members would not have provided and entrusted their Customer Data, including all information contained in the magnetic stripes of their credit and debit cards, to Forever 21 to eat at its restaurants and make purchases in the absence of the implied contract between them and Forever 21.

239. Plaintiffs and Class members fully performed their obligations under the implied contracts with Forever 21.

240. Forever 21 breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect the Customer Data of Plaintiffs and Class members and by failing to provide timely and accurate notice to them that their Customer Data was compromised as a result of the Data Breach.

241. Plaintiffs and Class members conferred a monetary benefit on Forever 21. Specifically, they purchased goods and services from Forever 21 and provided Forever 21 with their payment information. In exchange, Plaintiffs and Class members should have received from Forever 21 the goods and services that were the subject of the transaction and should have been entitled to have Forever 21 protect their Customer Data with adequate data security.

242. Forever 21 knew that Plaintiffs and Class members conferred a benefit on Forever 21 and accepted and has accepted or retained that benefit. Forever 21 profited from the purchases and used the Customer Data of Plaintiffs and Class members for business purposes.

243. Forever 21 failed to secure the Customer Data of Plaintiffs and Class members and, therefore, did not provide full compensation for the benefit the Plaintiffs and Class members provided.

244. Forever 21 acquired the Customer Data through inequitable means it failed to disclose the inadequate security practices previously alleged.

245. If Plaintiffs and Class members knew that Forever 21 would not secure their Customer Data using adequate security, they would not have made purchases at Forever 21.

246. Under the circumstances, it would be unjust for Forever 21 to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on it. Thus, Plaintiffs and Class members are entitled to restitution for the amounts by which Forever 21 has been unjustly enriched.

247. Forever 21 should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that it unjustly received from them.

248. As a direct and proximate result of Forever 21's breaches of the implied contracts between Forever 21 and Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages, including nominal damages, as described in detail above. This breach of the implied contracts was a direct and legal cause of the injuries and damages to Plaintiffs and members of the Class as described above.

249. Plaintiffs and the Class members were harmed as the result of Defendants' breach of the implied contracts because their PII and PCD were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII and PCD was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees, and other expenses relating to identity theft losses or protective measures. The Class members are further damaged as their PII remains in the hands of those who obtained it without their consent.

250. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiffs and Class members as described above.

Sixth Claim for Relief
Declaratory Judgment

251. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 130 as though fully stated herein.

252. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Forever 21 to provide adequate security for the PII and PCD it collected from their payment card transactions. As previously alleged, Forever 21 owes duties of care to Plaintiffs and Class members that require it to adequately secure PII and PCD.

253. Forever 21 still possesses PII and PCD pertaining to Plaintiffs and Class members. While the payment card account information may no longer be valid, because the bank has re-issued the card in the wake of the Data Breach, the PII remains valid as does the association and link between a person's personal identifying information and an account number once belonging to him or her.

254. Forever 21 has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its POS systems.

255. Accordingly, Forever 21 has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Forever 21's lax approach towards data security has become public, the Customer Data in its possession is more vulnerable than previously.

256. Actual harm has arisen in the wake of the Data Breach regarding Forever 21's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

257. Plaintiffs, therefore, seek a declaration that (a) Forever 21's existing data security measures do not comply with its contractual obligations and duties of care, and

(b) in order to comply with its contractual obligations and duties of care, Forever 21 must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Forever 21's systems on a periodic basis, and ordering Forever 21 to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Forever 21 is compromised, hackers cannot gain access to other portions of Forever 21 systems;

e. purging, deleting, and destroying in a reasonable secure manner Customer Data not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting 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. educating its 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 Forever 21 customers must take to protect themselves.

Seventh Claim for Relief
Violation of California's Customer Records Act – Inadequate Security
(Cal. Civ. Code § 1798.81.5) for the California subclass

258. Plaintiff Jowharah Hameed-Bolden repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 130 as though fully stated herein.

259. Plaintiff Hameed-Bolden brings this claim on behalf of herself and a California state subclass.

260. California Civil Code section 1798.80, *et seq.*, known as the "Customer Records Act" ("CRA") was enacted to "encourage business that own, license, or maintain personal information about Californians to provide reasonable security for that information." Cal. Civ. Code § 1798.81.5(a)(1).

261. Section 1798.81.5, subdivision (b) of the CRA requires any business that "owns, licenses, or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Under the CRA, "personal information" includes an individual's first name or first initial in combination with a social security number, driver's license number, account number or credit or debit card number and access code, medical information, or health insurance information. Cal. Civ. Code § 1798.82(h).

262. Forever 21 is a business that maintains personal information about California residents. As alleged in detail above, Defendants failed to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure," resulting in the Data Breach.

263. As the direct and legal result of Defendants' violation of section 1798.81.5, Plaintiff Hameed-Bolden and the members of the California subclass were harmed because their Customer Data compromised, placing them at a greater risk of identity theft and their Customer Data disclosed to third parties without their consent. Plaintiff Hameed-Bolden and Class members also suffered diminution in value of their Customer Data in that it is now easily available to hackers on the Dark Web. Plaintiff Hameed-Bolden and the California subclass have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. The California subclass members are further damaged as their Customer Data remains Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

264. Plaintiff Hameed-Bolden and the California subclass seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by Plaintiffs and the other class members as alleged above and equitable relief.

265. Defendants' misconduct as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiff Hameed-Bolden and the Class of "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiff Hameed-Bolden and the California subclass and despicable conduct that has subjected Plaintiff Hameed-Bolden and the California subclass to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff Jowharah Hameed-Bolden and the California subclass are entitled to punitive damages against Defendants under Civil Code § 3294(a).

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully requests that this Court enter an Order:

a. Certifying the Class and the California subclass, and Plaintiffs and their Counsel to represent the Class and subclass;

b. Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

c. Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

d. Awarding Plaintiffs and Class members actual, compensatory, consequential and/or nominal damages;

e. Awarding Plaintiffs and Class members statutory damages and penalties, as allowed by law;

f. Requiring Defendants to provide appropriate credit monitoring services to Plaintiffs and the other class members;

g. Compelling Defendants to use appropriate cyber security methods and policies with respect to data collection, storage and protection and to disclose with specificity to Class members the type of Customer Data compromised

h. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest;

i. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs and expenses, and;

j. Granting such other relief as the Court deems just and proper.

Dated: June 29, 2018

JOHN A. YANCHUNIS*
jyanchunis@ForThePeople.com
MARISA GLASSMAN*
mglassman@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

GLANCY PRONGAY & MURRAY LLP
KEVIN R. RUF (SBN 136901)
BRIAN P. MURRAY*
bmurray@glancylaw.com
GLANCY PRONGAY & MURRAY LLP
122 East 42nd Street, Suite 2920
New York, NY 10168
Telephone: (212) 682-5340

PAUL C. WHALEN *
paul@paulwhalen.com
LAW OFFICE OF PAUL C. WHALEN, P.C.
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870

JEAN SUTTON MARTIN*
jean@jsmlawoffice.com
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road Suite 225

Wilmington, NC 28403
Telephone: (910) 292-6676
Facsimile: (888) 316-3489

JASPER D. WARD IV*
jasper@jonesward.com
JONES WARD PLC
312 S. Fourth Street
Louisville, KY 40202
Telephone: (502) 882-6000

Attorneys for Plaintiffs and the Proposed Class

* *pro hac vice* application to be submitted