John A. Yanchunis (*Pro Hac Vice*)
jyanchunis@ForThePeople.com
Michael F. Ram (SBN 104805)
mram@forthepeople.com
Ryan J. McGee (*Pro Hac Vice*)
rmcgee@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
T: 813-223-5505
F: 813-223-5402 (fax)

Clayeo C. Arnold, California (SBN 65070)
carnold@justice4you.com
Joshua H. Watson, California (SBN 238058)
jwatson@justice4you.com
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
T: 916-777-7777
F: 916-924-1829

DANIEL L. WARSHAW (SBN 185365)
dwarshaw@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

MELISSA S. WEINER (*Pro Hac Vice*)
mweiner@pswlaw.com
JOSEPH C. BOURNE (SBN 308196)
jbourne@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610

Attorneys for Plaintiffs and the Proposed Class and Subclass (in the alternative)

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

MICHAEL FORD, NOE GAMBOA, and MADISON COPELAND, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

[24]7.AI, INC.,

Defendant.

CASE NO. 18-CV-02770-BLF
(related case no. 18-CV-05859)

SECOND CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

CLASS ACTION

JURY TRIAL DEMANDED

Plaintiffs, Madison Copeland ("Copeland"), Michael Ford ("Ford"), and Noe Gamboa ("Gamboa") (collectively, "Plaintiffs"), individually and on behalf of themselves and all others similarly situated, file this Second Consolidated Class Action Complaint against Defendant, [24]7.ai., Inc. ("Defendant" or "[24]7"), based upon personal knowledge with respect to themselves and on information and belief derived from the investigation of counsel and review of public documents as to all other matters, and allege as follows:

SUMMARY OF THE CASE

1. Plaintiffs bring this class action against Defendant for its failure to secure and safeguard customers' payment card data ("PCD") and other personally identifiable information ("PII") that Defendant collected while Plaintiffs and Class and Subclass members shopped on Best Buy's, Sears', and other companies' websites or chatted with customer service on Best Buy's, Sears', and other companies' websites in the Fall of 2017. Plaintiffs also brings this action against Defendant for its failure to provide timely, accurate, and adequate notice to Plaintiffs and Class and Subclass members that their PCD and PII (hereinafter, collectively, "Customer Data") had been compromised and stolen. Due to Defendant's introduction of security vulnerabilities to Best Buy, Sears, and other companies' websites and its failure to adequately secure Plaintiffs' and Class and Subclass members' Customer Data, their Customer Data was accessed by third parties without Plaintiffs' and Class and Subclass members' authorization (the "Data Breach").

2. Defendant is a customer experience software and services company headquartered in San Jose, California, with approximately 12,000 employees. Defendant offers sales and service-oriented software, as well as voice and chat agent services, for sales and support. Best Buy, Sears, and other companies have used Defendant for such services since at least, and likely well before, September 27, 2017—the purported beginning of the Data Breach described here.

3. In the years leading up to this Data Breach, retailers such as Target, Home Depot, Kmart, Wendy's, Neiman Marcus, and Brooks Brothers have experienced streams of attacks on their data security. Implementing measures to prevent those attacks, as well as quickly identifying them, has become a normal, expected part of the business.

4. On April 4, 2018, Sears announced that it had suffered a data breach caused by data

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

security failures relating to their use of Defendant's customer service chat services product.

5. On April 5, 2018, Best Buy acknowledged that customers who shopped online or used Best Buy's outsourced chat services for customer support were also potential victims of the Data Breach and their Customer Data was stolen.

6. This private Customer Data was compromised due to Defendant's acts and omissions and its failure to properly protect the Customer Data that became compromised through consumers' use of Best Buy's, Sears', and other companies' websites and the security vulnerabilities that Defendant introduced to those companies' websites.

7. Defendant could have prevented this Data Breach. Data breaches in the last few years have been the result of infiltration of computer systems in which Customer Data is exchanged. It is well known that cyber criminals seek access to this information to monetize it for illicit purposes and financial harm. While many retailers, restaurant chains, and other companies using such systems have responded to recent breaches by adopting technology and improving the security of their respective information environments that help make communication and transactions more secure, Defendant did not.

8. In addition to Defendant's failures to prevent the Data Breach, Defendant also failed to disclose the Data Breach for approximately six months, despite detecting and allegedly remedying the breach on October 12, 2017.[1]

9. The Data Breach was the inevitable result of Defendant's inadequate approach to data security and the protection of the Customer Data that it collected during the course of its business.

10. Defendant acknowledges that it collects personal information, including: first and last names; organization names; email addresses; phone numbers; physical addresses; dates of birth; gender; professional title; account information; credit/debit card numbers; and other information

[1] *[24]7.ai Issues Statement on Information Security*, PRNewswire (April 7, 2018) https://www.prnewswire.com/news-releases/247ai-issues-statement-on-information-security-300624659.html

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Defendant needs to provide client-specified services.[2] Indeed, Defendant claims to follow "industry standards to protect the security of End Users' Personal Information and Defendant respects End Users' choices for such information's intended use."[3] Defendant allegedly uses "a combination of reasonable and appropriate physical, technical, and administrative safeguards to prevent unauthorized access or disclosure of End Users' Personal Information," and claims that it "retains Personal Information and Interaction Data only as required or permitted by local law and while it has a legitimate business purpose."[4] Finally, Defendant represents that it "uses standard security protocols, and mechanisms to exchange the transmission of sensitive Personal Information such as credit card details and login credentials."[5]

11. Unfortunately, Defendant did not meet its security promises and obligations.

12. Instead, Defendant disregarded the rights of Plaintiffs and Class and Subclass members by: failing to take adequate and reasonable measures to ensure that its data systems were protected; failing to disclose to its clients (e.g., Best Buy and Sears) and those clients' customers the material fact that Defendant did not have adequate computer systems and security practices to safeguard Customer Data; failing to take available steps to prevent and stop the Data Breach from ever happening; failing to timely monitor and detect the Data Breach; and failing to timely notify Plaintiffs and Class and Subclass members of the Data Breach.

13. Through these actions and inactions, Defendant caused and exacerbated the damages Plaintiffs and Class and Subclass members suffered. If Defendant had detected the malware earlier and promptly notified Best Buy, Sears, Defendant's other clients, and the public of the Data Breach, the resulting losses would have been far less significant.

14. As a result of the Data Breach, the Customer Data of Plaintiffs and Class and Subclass members has been exposed to criminals for misuse—the very reason this information was

---

[2] *Platform Privacy Policy*, [24]7.ai, Inc., *available at* https://www.247.ai/privacy-policy#platform-policy (last visited Oct. 24, 2018).

[3] *Id.*

[4] *Id.*

[5] *Id.*

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

taken. As discussed in more detail below, the damages Plaintiffs and Class and Subclass members suffered as a direct result of the Data Breach include unauthorized charges on their debit or credit cards, theft of their personal and financial information, costs associated with the detection and prevention of identity theft, loss of access to their account funds and associated costs, time spent addressing these issues, and money paid for purchases with Defendant's clients that Plaintiffs and the Class and Subclass members otherwise would not have spent.

15. The damages to Plaintiffs and Class and Subclass members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for Customer Data.

16. The damages to Plaintiffs and Class and Subclass members were also directly and proximately caused by Defendant's failure to inform them that their Customer Data was subject to collection and storage by Defendant.

17. Plaintiffs retain significant interests in ensuring their respective Customer Data, which remains in the possession of Defendant, is protected from further breaches. Accordingly, they seek to remedy the harms they have suffered on behalf of themselves and other similarly situated consumers whose Customer Data was stolen and compromised as a result of the Data Breach.

18. Plaintiffs, on behalf of themselves and other 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

19. 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 Defendant.

20. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District, conducts substantial business in this District, and committed the acts and omissions complained of in the District.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

21. Venue is proper under 28 U.S.C. § 1391(c) because Defendant's 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 that that led to the Data Breach.

INTRADISTRICT ASSIGNMENT

22. This action arises in Santa Clara County, where Defendant is headquartered and where the relevant decisions and actions giving rise to the Data Breach occurred. Pursuant to Local Civil Rule 3-2(e), this action shall be assigned to the San Jose Division.

PARTIES

23. Plaintiff Madison Copeland is a resident of the state of Alabama.

24. Plaintiff Michael Ford is a resident of the state of Texas.

25. Plaintiff Noe Gamboa is a resident of the state of Illinois.

26. Defendant [24]7.ai is a California corporation that performs customer service functions for retailers and companies alike. Defendant's principal place of business and corporate headquarters is located in San Jose, Santa Clara County, California.

FACTUAL BACKGROUND

A. Plaintiff Copeland's Transactions

27. Plaintiff Copeland regularly makes purchases at Best Buy and other online retailers. For his purchases, he uses a credit card.

28. Between September 19, 2017, and October 17, 2017, Plaintiff Copeland made five purchases online through Best Buy's website, **www.bestbuy.com**. These purchases included a purchase on October 6, 2017, of computer and printer equipment and supplies.

29. On May 1, 2018, Plaintiff Copeland received a letter from Best Buy, which was titled, "NOTICE OF DATA BREACH" and dated April 25, 2018 (the "Notice Letter").

30. The Notice Letter advised Plaintiff Copeland that "we have determined that your personal information may have been affected by this incident." Best Buy blamed "malicious code that was inserted in" Defendant's software, which is used to provide Best Buy's customer service chat function. This allowed "an unauthorized party to access payment information of certain Best

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Buy customers who shopped on BestBuy.com" between September 26, 2017, and October 12, 2017. This information "included cardholder names, addresses and payment card information (including payment card number, expiration date and security code)." Best Buy claimed that it and Defendant had undertaken steps to try to fix the security flaws that had led to the data breach.

31. After reviewing the Notice Letter, Plaintiff Copeland spent approximately four hours researching the Data Breach and the security of his payment card information. Plaintiff Copeland works as a self-employed information technology contractor and bills his time at a rate of $50 per hour.

32. Plaintiff Copeland would not have used his payment card to make online purchases of merchandise from Best Buy had he known Defendant lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft. Thus, Plaintiff Copeland was injured by paying money for purchases of merchandise that he would not have made .

33. Plaintiff Copeland suffered injury from having his Customer Data compromised and stolen in the Data Breach.

34. Plaintiff Copeland also suffered injury in the form of damages to and diminution in the value of his Customer Data—a form of intangible property that he entrusted to Defendant, and which was compromised as a result of the Data Breach.

35. Plaintiff Copeland further suffered injury in the form of time spent dealing with the Data Breach.

36. Additionally, Plaintiff Copeland has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Customer Data being placed in the hands of criminals.

37. Moreover, Plaintiff Copeland has a continuing interest in ensuring that his private information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

B. Plaintiff Ford's Transactions

38. Plaintiff Ford regularly makes purchases at Best Buy and uses the online chat function to communicate with what he believed was Best Buy's customer service, but was in fact

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Defendant's technology. For his purchases, Plaintiff Ford uses a credit card.

39. Following the announcement of the Data Breach, Plaintiff Ford reviewed his financial statements and identified fraudulent activity in the amount of $370. Due to this fraudulent activity, he activated a fraud alert, froze his credit card account, and requested a replacement from his financial institution.

40. Plaintiff Ford would not have used his payment card to make online purchases of merchandise from Best Buy had he known Defendant lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

41. Plaintiff Ford suffered injury from having his Customer Data compromised and stolen in the Data Breach.

42. Plaintiff Ford also suffered injury in the form of damages to and diminution in the value of his Customer Data—a form of intangible property that he entrusted to Defendant, and which was compromised as a result of the Data Breach.

43. Plaintiff Ford further suffered injury in the form of time spent dealing with the Data Breach.

44. Additionally, Plaintiff Ford has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Customer Data being placed in the hands of criminals.

45. Moreover, Plaintiff Ford has a continuing interest in ensuring that his private information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

C. Plaintiff Gamboa's Transactions

46. Plaintiff Gamboa regularly makes purchases at Best Buy and uses the online chat function to communicate with what he believed was Best Buy's customer service, but was in fact Defendant's technology. For his purchases, Plaintiff Gamboa uses a credit card.

47. Plaintiff Gamboa's financial institution alerted him to, and he identified, fraudulent activity related to an attempted purchase of merchandise with his payment card, which is the same payment card Plaintiff Gamboa used to purchase goods from Best Buy during the Data Breach.

48. Similar to Plaintiff Copeland, Plaintiff Gamboa received the Notice Letter from Best Buy, informing him that his Customer Data had been compromised.

49. Plaintiff Gamboa would not have used his payment card to make online purchases of merchandise from Best Buy had had he known Defendant lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

50. Plaintiff Gamboa suffered injury from having his Customer Data compromised and stolen in the Data Breach.

51. Plaintiff Gamboa also suffered injury in the form of damages to and diminution in the value of his Customer Data—a form of intangible property that he entrusted to Defendant, and which was compromised as a result of the Data Breach.

52. Plaintiff Gamboa further suffered injury in the form of time spent dealing with the Data Breach.

53. Additionally, Plaintiff Gamboa has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Customer Data being placed in the hands of criminals.

54. Moreover, Plaintiff Gamboa has a continuing interest in ensuring that his private information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

D. Defendant Collects and Stores Customer Data for Its Own Financial Gain

55. Founded in 2000,[6] Defendant operates a variety of customer services products with artificial intelligence technologies from its offices in San Jose, California, with additional offices in Toronto, London, Stockholm, and Sydney, and numerous clients in retail, education, financial services, healthcare, insurance, travel and hospitality, and utilities.[7]

56. Since its founding, Defendant has aggressively expanded, including private funding from Sequoia Capital—a venture capital firm controlling $1.4 trillion in assets—in 2003, as well as a partnership with Microsoft in 2012, in which Microsoft combined its "interactive self-service assets" with Defendant's technologies.[8]

57. At all relevant times, Defendant was aware, or reasonably should have been aware, that the Customer Data collected, maintained, and stored in Defendant's computer systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

58. 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, Defendant maintained an insufficient and inadequate system to protect Plaintiff's and Class members' Customer Data.

59. Customer Data is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber black market" exists in which criminals openly post stolen payment card numbers, and other personal information on the internet, including the dark web. Customer Data is valuable 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.

---

[6] *[24]7.ai Company Profile*, Forbes, https://www.forbes.com/companies/24-7/ (last visited Oct. 24, 2018).

[7] *[24]7.ai Company Overview*, Bloomberg, *available at* https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=4532786 (last visited Oct. 24, 2018)

[8] *Microsoft picks stake in Sequoia-backed [24]7.ai Inc*, Reuters (Feb. 9, 2012) https://in.reuters.com/article/microsoft-picks-stake-in-sequoia-backed-idINDEE81807U20120209

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

60. 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."[9]

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on consumers as a result of a data breach.

62. Defendant was, or reasonably should have been, fully aware of the significant volume of daily credit and debit card transactions and PII provided in customer service interactions and purchases and, thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

63. Despite all of this publicly available knowledge of the continued compromises of Customer Data in the hands of other third parties, such as retailers, Defendant's approach to maintaining the privacy and security Plaintiff's and Class members' Customer Data was inadequate and unreasonable.

E. Defendant Had Notice of Data Breaches Involving Malware on POS Systems

64. Prior to Defendant's Data Breach, a wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[10] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a 40% increase in the number of data breaches from the previous year.[11] The amount of payment card data compromised by data breaches

---

[9] *Verizon 2014 PCI Compliance Report*, Verizon, *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 Oct. 24, 2018).

[10] *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

[11] *Id*.

is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[12]

65. Many of the data breaches occurring within the last several years involved malware placed on computer systems that retail merchants and their agents use.

66. These data breaches involve compromising payment systems at physical retail outlets, phishing schemes to gain access to internal servers and information, and exploiting other vulnerabilities in companies' websites and electronically stored data systems.

F. The Data Breach

67. On April 4, 2018, Delta and Sears announced that that the Data Breach had compromised their customers' information. The Customer Data was stolen as a result of security vulnerabilities introduced by the companies' use of Defendant's software and technology.

68. Best Buy announced the Data Breach on April 5, 2018. According to its statements, Best Buy was informed of the Data Breach on March 28, 2018. The Customer Data was stolen as a result of security vulnerabilities introduced by the companies' use of Defendant's software and technology.

69. Defendant possibly knew of the Data Breach as early as September 26, 2017, when the Data Breach allegedly began, and definitively on October 12, 2017—when Defendant allegedly fixed the security issues.[13]

70. Despite knowing of the Data Breach since at least October 12, 2017, Defendant has not provided any details regarding the degree and extent of the Data Breach—even though it handles chat services for Best Buy, Sears, and several other large companies.

---

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

[13] *Updates on [24]7.ai Cyber Incident: Statement from [24]7.ai*, Best Buy, https://www.bestbuy.com/site/privacy-policy/247-ai-cyber-incident/pcmcat1522954594900.c?id=pcmcat1522954594900 (last updated April 13, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

71. Worse, Defendant's "Resource Center"[14] provides no updates or additional details regarding the Data Breach, and any attempts a consumer takes to search for updates in Defendant's "Resource Center" with basic terms such as "data breach," "breach," "incident," "Best Buy," "Sears," and other descriptors relevant to this and a generic data breach are met with "No resources found!" in the results, leaving consumers with no updates or additional details regarding the Data Breach and the efforts to secure and protect Plaintiffs' and Class and Subclass members' Customer Data.

72. Curiously, since the passage of time between the Data Breach and this case's litigation history, 24[7] has entirely scrubbed its resource and news centers of *any news* predating August 22, 2018.[15] Indeed, when consumers visit the initial press release from PRNewswire and follow the hyperlink to "24[7].ai," the page is devoid of any content concerning the Data Breach, but touts 24[7]'s accomplishments in acquiring a new Chief Financial Officer and Chief Data Scientist; that its Chief Revenue Officer was recognized as a "sales transformation expert," and other technological advances in its product, but nothing concerning the security of [24]7's service.[16]

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

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

74. The ramifications of Defendant's failure to keep Plaintiffs' and Class and Subclass members' Costumer Data secure are severe.

75. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[17] The FTC describes "identifying

---

[14] *Resource Center*, [24]7.ai, Inc., *previously available at* https://www.247.ai/resource-center (last visited Oct. 24, 2018).

[15] *Press Releases*, [24]7.ai, Inc., *available at* https://www.247.ai/company/press-releases (last visited September 23, 2018)

[16] *Id.*

[17] 17 C.F.R § 248.201 (2013).

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[18]

76. PII 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."[19]

77. Identity thieves can use personal information 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; 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.

78. Identity thieves have stolen $112 billion from 2010 to February 2016,[20] with that figure drastically increasing due to the frequency and magnitude of additional data breaches—including this and others—in the months and years since Javelin Strategy issued its report.

79. 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 DOJ 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.[21]

---

[18] *Id.*

[19] Federal Trade Commission, Consumer Information, *Warning Signs of Identity Theft*, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Oct. 24, 2018).

[20] *See* Al Pascual, et al., *2016 Identity Fraud: Fraud Hits an Inflection Point*, Javelin Strategy (Feb. 2, 2016) https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point

[21] Erika Harrell, *Victims of Identity Theft, 2014*, Department of Justice, Office of Justice Programs, http://www.bjs.gov/content/pub/pdf/vit14.pdf (last revised Nov. 13, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

80. There may be a time lag between when harm occurs and 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.[22]

81. Plaintiffs and Class and Subclass members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class and Subclass members are 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.

H. Plaintiffs and Class and Subclass Members Suffered Damages

82. Plaintiffs' and Class and Subclass members' Customer Data is private and sensitive in nature, and Defendant left that Customer Data inadequately protected and caused it to be inadequately protected. Defendant did not obtain Plaintiffs' and Class and Subclass members' consent to disclose their Customer Data to any other person, as required by applicable law and industry standards.

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

---

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

84. Defendant had the resources to prevent a breach. For example, Defendant is funded by Sequoia Capital and partners with Microsoft.

85. Had Defendant employed security measures recommended by experts in the field, Defendant would have prevented intrusion into their computer systems and, ultimately, the theft of its client's customers' Customer Data.

86. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class and Subclass members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud. This increased risk requires Plaintiffs and Class and Subclass members to take the time (which they otherwise could have dedicated to other life demands, such as work or personal endeavors) and effort to mitigate the actual and potential impact of the Data Breach, including by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts and passwords, 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 negligent or unlawful conduct, as is the case here.

87. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class and Subclass 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 Customer Data being placed in the hands of criminals;

d. the improper disclosure of their Customer Data;

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

e. loss of privacy;

f. the monetary amount of purchases at Best Buy, Sears, and other companies Defendant serviced during the period of the Data Breach that Plaintiffs and Class and Subclass members would not have made had they known adequate systems and procedures to reasonably protect their Customer Data were absent;

g. 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;

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

i. 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;

j. 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

k. the loss of productivity and value of their time spent to attempt to address the actual and future consequences of the Data Breach, including finding fraudulent charges; canceling 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.

88. Defendant has not offered credit monitoring or identity theft protection services to any affected customers directly. Even retailers have not offered *adequate* credit monitoring or identity theft protection services. For instance, Best Buy stated that it will offer credit monitoring or identity theft protection services limited to one year, even though criminals can and often do simply sit on the stolen Customer Data for more than one year and then misuse it. As a result, Plaintiffs

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

and Class and Subclass members are left to their own actions to adequately protect themselves from the financial damage Defendant has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Defendant's actions have created for Plaintiffs and Class and Subclass members is ascertainable and is a determination appropriate for the trier of fact.

89. While Plaintiffs' and Class and Subclass members' Customer Data has been stolen, Defendant continues to hold Customer Data of consumers, including Plaintiffs and Class and Subclass members. Because Defendant has demonstrated an inability to prevent a breach or promptly stop it, Plaintiffs and Class and Subclass members have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

90. Some merchants have arrangements with credit card processors, such as Visa and Mastercard, to allow authorization for expired payment cards.[23] Thus, even though payment card data may be expired or replaced, a hacker, scammer, or other nefarious actor may be able to use an expired or replaced payment card account from a data breach to conduct transactions long after the data breach.

91. Some merchants have arrangements with credit card processors to update Customer Data, in particular payment card information within the merchant account, automatically when a new card is issued by the processor.[24] Thus, if a hacker, scammer, or other nefarious actor has used a stolen payment card to open a merchant account using the cardholder's Customer Data, the card information in the fraudulent account may be updated automatically when the card is reissued after a data breach and card cancellation.

CHOICE OF LAW

---

[23] See, Lifehacker, *How Scammers Can Use Your Old Credit Card Numbers* (Jan. 6, 2020), available at https://twocents.lifehacker.com/how-scammers-can-use-your-old-credit-cardnumbers-1840513053.

[24] Credit.com, *How Companies Know Your New Credit Card Number Before You Give It To Them* (July 15, 2016), available at https://www.credit.com/blog/2016/07/how-companies-knowyour-new-credit-card-number-before-you-give-it-to-them-151126/.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

92. Defendant is incorporated and headquartered in San Jose, California. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

93. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's California headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Data Breach were made from and in California. Finally, Defendant's breach of its duty to customers—including Plaintiffs and Class and Subclass members—emanated from California.

94. It is appropriate to apply California law extraterritorially to the claims against Defendant in this case due to Defendant's significant contacts with California. Defendant is headquartered in California; the relevant decisions, actions, and omissions were made in California; and Defendant cannot claim to be surprised by application of California law to regulate its conduct emanating from California.

95. To the extent California law conflicts with the law of any other state that could apply to Plaintiffs' claims against Defendant, application of California law would lead to the most predictable result, promote the maintenance of interstate order, simplify the judicial task, and advance the forum's governmental interest.

CLASS ACTION ALLEGATIONS

96. 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 on behalf of the proposed nationwide class (the "Class") defined as follows:

> All persons who use Defendant's electronic customer service platform or who shopped on Best Buy's, Sears', or any other of Defendant's clients' websites or mobile applications, and whose Customer Data was compromised as a result of the Data Breach.

97. Pursuant to Rule 23(b)(2), (b)(3), and (c)(4), Plaintiff Gamboa seeks certification of state claims (Count IV for violation of the Illinois Consumer Fraud and Deceptive Business Practices

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Act) in the alternative to the nationwide claims on behalf of a separate Illinois statewide subclass (the "Illinois Subclass") defined as follows:

> All persons who reside in Illinois and use Defendant's electronic customer service platform or who shopped on Best Buy's, Sears', or any other of Defendant's clients' websites or mobile applications, and whose Customer Data was compromised as a result of the Data Breach.

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

99. **Numerosity:** The members of the Class and Subclass are so numerous that joinder of all Class and Subclass members would be impracticable. Plaintiffs reasonably believe that Class and Subclass members number in the hundreds of thousands of people or more in the aggregate. The names and addresses of Class and Subclass members are identifiable through documents Defendant and third parties (such as Best Buy and Sears) maintain.

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

a. Whether Defendant owed a legal duty to Plaintiffs and Class and Subclass members to exercise due care in collecting, storing, and safeguarding their Customer Data;

b. Whether Defendant breached a legal duty to Plaintiffs and Class and Subclass members to exercise due care in collecting, storing, and safeguarding their Customer Data;

c. Whether Defendant knew or should have known of the susceptibility of its computer systems to a data breach;

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

d. Whether Defendant knew or should have known of the susceptibility it caused in Best Buy's, Sears', and other of Defendant's clients' computer systems to a data breach;

e. Whether Defendant's security measures to protect its computer systems were reasonable in light of industry data security standards and recommendations;

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

g. Whether Plaintiffs' and Class and Subclass members' Customer Data was accessed, exposed, compromised, or stolen in the Data Breach;

h. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

i. Whether Defendant's failure to implement adequate data security measures allowed the breach of their computer systems to occur;

j. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of Plaintiffs' and Class and Subclass members' Customer Data;

k. Whether Defendant failed to timely notify the public of the Data Breach;

l. Whether Defendant's conduct constituted deceptive trade practices;

m. Whether Defendant's conduct violated California's Unfair Competition Law;

n. Whether Defendant's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;

o. Whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act;

p. Whether Plaintiffs and Class and Subclass members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

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

101. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of Class and Subclass members. 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.

102. **Typicality:** Plaintiffs' claims are typical of Class and Subclass members' claims because, among other things, Plaintiffs and Class and Subclass members were injured through Defendant's substantially uniform misconduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and Class and Subclass members, and there are no defenses that are unique to Plaintiffs' claims. Plaintiffs' and Class and Subclass members' claims arise from the same operative facts and are based on the same legal theories.

103. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class and Subclass because their interests do not conflict with the interests of the other Class and Subclass members they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation, including data privacy and data security practices litigation; and Plaintiffs will prosecute this action vigorously for the benefits of the Class and Subclass. Class and Subclass members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

104. **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 Class and Subclass members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class and Subclass members to individually seek redress for Defendant's wrongful conduct. Even if Class and Subclass members could afford individual litigation, the court system could not. Individualized litigation would create a potential

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

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.

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

106. 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 the Class and Subclass members' Customer Data was accessed, exposed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendant knew about the Data Breach before it was announced to the public and whether Defendant failed to timely notify the public of the Data Breach;

c. Whether Defendant misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and the Class and Subclass members' Customer Data;

d. Whether Defendant concealed crucial information about its inadequate data security measures from Plaintiffs and Class and Subclass members;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

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

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class and Subclass members' Customer Data in violation of Section 5 of the FTC Act;

i. Whether Defendant failed to provide timely notice of the Data Breach, to Plaintiffs and Class and Subclass members;

j. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;

k. Whether Defendant's conduct violated 815 Ill. Comp. Stat. Ann. §§ 505, *et seq.*;

l. Whether Defendant's conduct Or. Rev. Stat. §§ 646.605, *et seq.*;

m. Whether Defendant's conduct Or. Rev. Stat. §§ 646A.604, *et seq.*;

n. Whether Defendant owed a duty to Plaintiffs and Class and Subclass members to safeguard their Customer Data and to implement adequate data security measures;

o. Whether Defendant failed to adhere to its posted privacy policies concerning the care it would take to safeguard Plaintiffs' and Class and Subclass members' Customer Data in violation of Cal. Bus. & Prof. Code § 22576;

p. Whether Defendant negligently and materially failed to adhere to its posted privacy policies concerning the safeguarding of Plaintiffs' and Class and Subclass members' Customer Data in violation of Cal. Bus. & Prof. Code § 22576;

q. Whether Defendant breached those duties.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

CLAIMS ALLEGED ON BEHALF OF THE CLASS

First Claim for Relief
Negligence
On Behalf of All Plaintiffs and the Class

107. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 106 as though fully stated herein.

108. Plaintiffs bring this claim on behalf of themselves and the Class.

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

110. Defendant owed a duty of care not to subject Plaintiffs and all 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.

111. Defendant owed a duty to Plaintiffs and all Class members 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 Defendant's security systems to ensure Plaintiffs' and all Class members' Customer Data was adequately secured and protected. Defendant further had a duty to implement processes that would detect a breach of their data system in a timely manner.

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

113. By being entrusted by Plaintiffs and all Class members to safeguard their respective Customer Data, Defendant had special relationships with Plaintiffs and all Class members. Plaintiffs

and all Class members made purchases through Best Buy's, Sears', and other of Defendant's clients' websites and/or utilized Defendant's customer service chat product with the understanding that Defendant would take appropriate measures to protect their Customer Data and would inform Plaintiffs and all Class members of any breaches or other security concerns that might call for action. But Defendant did not. Defendant not only knew its data security was inadequate, it also knew it did not have the tools to detect and document intrusions or exfiltration of Customer Data. Defendant is morally culpable, given its wholly inadequate safeguards, as well as its refusal to notify Plaintiffs and all Class members of breaches or security vulnerabilities.

114. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and all Class members' Customer Data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, and allowing unauthorized access to Plaintiffs' and all Class members' Customer Data.

115. Defendant also breached its duty to timely disclose that Plaintiffs' and all Class members' Customer Data had been, or was reasonably believed to have been, stolen, exposed, or compromised.

116. Defendant's failure to comply with industry standards further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and all Class members' Customer Data.

117. But for Defendant's respective wrongful and negligent breach of its duty owed to Plaintiffs and all Class members, their Customer Data would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's respective negligence was a direct and legal cause of the theft of Plaintiffs' and all Class members' Customer Data, as well as the resulting damages.

118. The injury and harm Plaintiffs and all Class members suffered was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and all Class members' Customer Data. Defendant knew its computer systems and technologies for accepting and securing Plaintiffs' and all Class members' Customer Data had numerous security vulnerabilities.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

119. As a result of Defendant's misconduct, Plaintiffs' and all Class members' Customer Data 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 all 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 all Class members 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.

120. Having substantiated a claim of ordinary negligence, Plaintiffs are entitled to a presumption of negligence *per se*, based upon Defendant's violations of the FTC Act, which are evidence of its negligence.

121. Section 5(a) of the FTC Act prohibits "unfair … practice in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by business, such as Defendant, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described in this complaint also form part of the basis of Defendant's duties in this regard.

122. Defendant violated Section 5(a) of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and all Class members' Customer Data and not complying with applicable industry standards, as described in detail above. Defendant's conduct was particularly unreasonable given the nature and amount of Customer Data that Defendant stored, and the foreseeable consequences of a data breach including, specifically, the immense damages that would result to Plaintiffs and all Class members.

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

124. 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 Plaintiffs and all Class members suffered.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

125. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and all Class members have suffered, and continue to suffer, injuries and damages arising from Plaintiffs' and the Class members' 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.

Second Claim for Relief

Violation of California's Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)
On Behalf of All Plaintiffs and the Class

126. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 106 as though fully stated herein.

127. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200 *et seq.*

128. Defendant stored the Customer Data of Plaintiffs and all Class members in its computer systems. Defendant falsely represented to Plaintiffs and all Class members that their Customer Data was secure and would remain private.

129. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiffs and all Class members' Customer Data secure and prevented the loss or misuse of that Customer Data.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

130. Even without these misrepresentations, Plaintiffs and all Class members were entitled to assume, and did assume, that Defendant would take appropriate measures to keep their Customer Data safe. Defendant did not disclose at any time that Plaintiffs' and all Class members' Customer Data was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

A. Unlawful Business Practices

131. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, both by affirmative conduct and by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiffs' and all Class members' Customer Data.

132. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, and by failing to immediately notify Plaintiffs and all Class members of the Data Breach.

133. If Defendant had complied with these legal requirements, Plaintiffs and all Class members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiffs and all Class members of the Data Breach.

134. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act.

135. Plaintiffs and all Class members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In particular, Class members have suffered from fraudulent charges to their credit/debit card accounts as a result of the Data Breach. In addition, Plaintiffs and all Class members' Customer Data 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. Plaintiffs and all Class members 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.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

B. Unfair Business Practices

136. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and misrepresentations to consumers about Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and all Class members, directly causing the harms alleged below.

137. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's 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."). Defendant's acts and omissions thus amount to a violation of the law.

138. **Defendant engaged in unfair business practices under the "FTC test."** The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects hundreds of thousands of Class members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiffs' and all 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 Plaintiffs' and all Class members' Customer Data remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

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"); *see also, e.g.*, *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).

139. Plaintiffs and all Class members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. In particular, Class members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, Plaintiffs and all Class members' Customer Data 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. Plaintiffs and all Class members 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.

140. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiffs and all Class members are entitled to injunctive relief and reasonable attorneys' fees and costs.

Third Claim for Relief

Breach of Confidence
On Behalf of All Plaintiffs and the Class

141. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 106 as though fully stated herein.

142. This claim is asserted against Defendant for breach of confidence concerning the Customer Data Plaintiffs and all Class Members provided to Defendant in confidence.

143. At all times during Plaintiffs' and Class and Subclass members' interactions with Defendant, Defendant was fully aware of the confidential nature of the Customer Data that Plaintiffs and all Class members shared with Defendant.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

144. As alleged herein and above, Defendant's relationship with Best Buy, Sears, and other clients were governed by terms and expectations that Plaintiffs' and Class and Subclass members' Customer Data would be collected, stored, and protected in confidence, and not disclosed to unauthorized third parties.

145. Plaintiffs and all Class Members provided their respective Customer Data to Defendant with the explicit and implicit understanding that Defendant would protect and not permit the Customer Data to be disseminated to any unauthorized third parties.

146. Plaintiffs and all Class Members also provided their respective Customer Data to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect the Customer Data from unauthorized disclosure, such as following basic principles of encryption and information security practices.

147. Defendant voluntarily received in confidence Plaintiffs' and all Class members' Customer Data with the understanding that Customer Data would not be disclosed or disseminated to the public or any unauthorized third parties.

148. Due to Defendant's failure to prevent, detect, and stop the Data Breach from occurring, Plaintiffs' and all Class members' Customer Data was disclosed and misappropriated to the public and unauthorized third parties beyond Plaintiffs' and all Class members' confidence and without their express permission.

149. As a direct and proximate cause of Defendant's actions and inactions, Plaintiffs and all Class members have suffered damages.

150. But for Defendant's disclosure of Customer Data in violation of the parties' understanding of confidence, their Customer Data would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's disclosure was the direct and legal cause of the theft of Plaintiffs' and all Class members' Customer Data, as well as the resulting damages.

151. The injury and harm Plaintiffs and all Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and all Class members' Customer Data. Defendant knew its computer systems and technologies for accepting and securing Plaintiffs' and all Class members' Customer Data had numerous security vulnerabilities because

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Defendant failed to observe even basic information security practices or correct known security vulnerabilities.

152. As a result of Defendant's misconduct, Plaintiffs' and all Class members' Customer Data 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 all 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 all Class members 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.

Fourth Claim for Relief

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (815 Ill. Comp. Stat. Ann. §§ 505, *et seq.*)
Pled in the alternative and on Behalf of Plaintiff Gamboa and the Illinois Subclass

153. Plaintiff Gamboa repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 106 as though fully stated herein.

154. Plaintiff Gamboa brings this cause of action in the alternative to a nationwide class.

155. Defendant is a "person" pursuant to 815 Ill. Comp. Stat. Ann. § 505/1(c).

156. Plaintiff Gamboa and the Illinois Subclass are "consumer[s]" pursuant to 815 Ill. Comp. Stat. Ann. § 505/1(e).

157. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" pursuant to 815 Ill. Comp. Stat. Ann. § 505/1(f).

158. Defendant's deceptive, unfair, and unlawful trade acts or practices violate 815 Ill. Comp. Stat. Ann. § 505/2.

159. Defendant's representations and omissions concerning the handling, storing, and securing of Plaintiff Gamboa's and the Illinois Subclass members' Customer Data were material because those representations and omissions were likely to deceive reasonable consumers to believe their Customer Data could be and was kept private.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

160. Defendant intended to mislead Plaintiff Gamboa and the Illinois Subclass members and induce them to rely on its misrepresentations and omissions. Plaintiff Gamboa and the Illinois Subclass members reasonably relied on Defendant's representations and omissions concerning the handling, storing, and securing of Plaintiff Gamboa's and the Illinois Subclass members' Customer Data.

161. Defendant's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts and practices caused substantial injury that Plaintiff Gamboa and the Illinois Subclass members could not reasonably avoid; this substantial injury outweighed any benefit to consumers or competition.

162. Defendant acted intentionally, knowingly, and maliciously to violate Illinois' Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiff Gamboa's and the Illinois Subclass members' rights.

163. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff Gamboa and the Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money and property, and monetary and non-monetary damages. These damages include improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, Plaintiff Gamboa's and the Illinois Subclass members' Customer Data 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. Plaintiff Gamboa and the Illinois Subclass members 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.

164. Plaintiff Gamboa and the Illinois Subclass members have suffered injuries in fact and lost money or property due to Defendant's deceptive, unfair, and unlawful trade acts or practices. Plaintiff Gamboa's and the Illinois Subclass members' Customer Data has tangible value and is now in the possession of third parties who have used and will use it for their own advantage, including financial advantage, and is being sold for value, making it clear that the Customer Data has tangible value.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

165. Plaintiff Gamboa and the Illinois Subclass members are at increased risk of identity theft due to Defendant's deceptive, unfair, and unlawful trade acts or practices and failure to properly protect Plaintiff Gamboa's and the Illinois Subclass members' Customer Data. Plaintiff Gamboa and the Illinois Subclass members are now subject to identity theft, medical fraud, and other concrete harms. The Customer Data Defendant permitted third parties to access allows that Customer Data to be aggregated with other data to identify and target Plaintiff Gamboa and the Illinois Subclass members. It is reasonable for Plaintiff Gamboa and the Illinois Subclass members to obtain identity protection and credit monitoring services in light of the foregoing. Plaintiff Gamboa and the Illinois Subclass members seek to recover the cost of these services from Defendant because of Defendant's deceptive, unfair, and unlawful trade acts or practices.

JURY TRIAL DEMANDED

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of Class and Subclass members, respectfully request that this Court enter an Order:

a. Certifying the Class and Subclass, and appointing Plaintiffs and their Counsel to represent the Class and the Subclass;

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

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

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

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

f. Requiring Defendant to provide appropriate credit monitoring services to Plaintiffs and Class and Subclass members;

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

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

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

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

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

Dated: September 26, 2020

/s/ *John A. Yanchunis*
John A. Yanchunis

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

John A. Yanchunis (*Pro Hac Vice*)
jyanchunis@ForThePeople.com
Ryan J. McGee (*Pro Hac Vice*)
rmcgee@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
T: 813-223-5505
F: 813-223-5402 (fax)

Michael F. Ram (SBN 104805)
mram@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Ave., Suite 500
San Francisco, CA 94102

Clayeo C. Arnold, California (SBN 65070)
carnold@justice4you.com
Joshua H. Watson, California (SBN 238058)
jwatson@justice4you.com
CLAYEO C. ARNOLD, A
PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
T: 916-777-7777
F: 916-924-1829

DANIEL L. WARSHAW (SBN 185365)
dwarshaw@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

MELISSA S. WEINER (*Pro hac vice*)
mweiner@pswlaw.com
JOSEPH C. BOURNE (SBN 308196)
jbourne@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, MN 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610

Attorneys for Plaintiffs and the Proposed Class