FARUQI & FARUQI, LLP
Benjamin Heikali (State Bar No. 307466)
Email: *bheikali@faruqilaw.com*
Ruhandy Glezakos (SBN 307473)
Email: *rglezakos@faruqilaw.com*
Joshua Nassir (State Bar No. 318344)
Email: *jnassir@faruqilaw.com*
10866 Wilshire Boulevard, Suite 1470
Los Angeles, California 90024
Telephone: (424) 256-2884
Facsimile: (424) 256-2885

[*additional counsel on signature page]*

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

ERIK SOLTER, and LORNE BULLING, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SPORTS WAREHOUSE, a California corporation d/b/a TENNIS WAREHOUSE; RUNNING WAREHOUSE, LLC; WILDERNESS SPORTS WAREHOUSE LLC d/b/a TACKLE WAREHOUSE; and SKATE WAREHOUSE, LLC,

Defendants.

Case No. 2:22-cv-00460

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Erik Solter and Lorne Bulling (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, by and through their undersigned counsel, hereby file this Class Action Complaint against Sports Warehouse d/b/a Tennis Warehouse ("Tennis Warehouse"), Running Warehouse, LLC ("Running Warehouse"), Wilderness Sports Warehouse d/b/a Tackle Warehouse ("Tackle Warehouse"), and Skate Warehouse, LLC ("Skate Warehouse") (collectively, "Defendants," or the "Companies").

NATURE OF THE ACTION

1. This is a data breach class action on behalf of Defendants' customers whose payment card information was stolen by cybercriminals as part of a cyber-attack on Defendants' payment card environment and systems. Hackers infiltrated and accessed the Company's inadequately protected payment card environment and systems on October 1, 2021, during which time they gained illegitimate access to customer data for four (4) affiliated sports gear online shopping websites operated by Defendants (tacklewarehouse.com, runningwarehouse.com, tennis-warehouse.com, and skatewarehouse.com). The threat actors were able to obtain the protected personal information of more than 1.8 million customers of Defendants by accessing Defendants' payment card environment and computer systems and stealing customers' personally identifiable information including payment card information ("PII"). The PII that was obtained reportedly included customers' full names, financial account numbers, credit and debit card numbers with CVVs, and website login credentials (the "Data Breach").[1]

[1] *See Hackers Pilfer Credit Card Info of 1.8 Mn People from 4 Sports Gear Sites!*, https://www.stealthlabs.com/news/hackers-pilfer-credit-card-info-of-1-8-mn-people-from-4-sports-gear-sites/ (last accessed January 21, 2022); *Credit card info of 1.8* (footnote continued)

2. The Companies reportedly first learned of the breach on October 15, 2021, and after an investigation, confirmed on November 29, 2021, which customers had their payment information stolen.

3. On information and belief, the threat actors stole the PII of more than 1.8 million customers of Defendants.

4. According to Defendants' notice to state attorneys general advising of the Data Breach, Defendants reportedly became aware of a potential data security incident on October 15, 2021 but did not determine that payment card information was obtained until November 6, 2021 and did not advise affected individuals of the Data Breach until December 16, 2021, two and a half (2 1/2) months after the Data Breach occurred.

5. On or about December 16, 2021, Defendants began mailing breach notifications to affected customers. According to the notice letter Defendants sent to affected individuals, Defendants identified suspicious activity on their computer systems on October 15, 2021 and opened an internal investigation. Defendants' investigation determined the Companies suffered a "data security incident" on October 1, 2021, when highly sensitive customer payment card information was obtained without authorization.

6. On information and belief, Plaintiffs' and Class members' PII was stolen in the cyberattack. Plaintiffs' and Class members' PII has already been and will continue to be used for criminal purposes, such as identity theft and fraudulent

---

million people stolen from sports gear sites, https://www.bleepingcomputer.com/news/security/credit-card-info-of-18-million-people-stolen-from-sports-gear-sites/ (last accessed January 21, 2022); and *Hackers steal credit cards from 1.8 million sports gear site customers*, https://www.bitdefender.com/blog/hotforsecurity/hackers-steal-credit-cards-from-1-8-million-sports-gear-site-customers/ (last accessed January 21, 2022).

purchases and sold by the actors responsible for the Data Breach to other criminals on the dark web.

7. Defendants' conduct – failing to take adequate and reasonable measures to ensure that their customer data was protected, failing to take available steps to prevent and stop the Data Breach, failing to take adequate measures to detect the Data Breach, failing to provide timely notice of the Data Breach, and enabling the actors to execute the Data Breach and steal Plaintiffs' and Class members' PII – has caused substantial harm and injuries to their customers.

8. Defendants' material failures put Plaintiffs' and Class members' PII and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class members associated with time and money spent as a result of taking time and incurring costs to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach.

9. As a result of the Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their PII has been released into the criminal cyber domains, Plaintiffs and Class members are at imminent and impending risk of identity theft. Additionally, Plaintiffs and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

10. As a result of the Data Breach, many class members have experienced and will continue to experience fraudulent credit and debit card transactions and other fraud related to their accounts. Class members have incurred and will continue to incur out-of-pocket costs, including costs relating to purchasing protective measures such as credit monitoring services, credit freezes, and credit reports, bank fees, late fees, or other costs directly or indirectly related to the Data Breach.

11. As discussed in more detail below, Plaintiffs have sustained actual, palpable misuse of their payment cards and have suffered other types of injuries and

damages as a result of the Data Breach. Plaintiffs and Class members have also been exposed to a heightened and imminent risk of fraud and identity theft. In addition to the significant inconvenience the breach has already caused, Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against fraud. This is a burdensome and time-consuming process.

12. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose payment card information or PII was stolen in the Data Breach. Plaintiffs seek remedies including reimbursement of out-of-pocket losses, compensation for time spent in response to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief involving substantial improvements to Defendants' card payment data security systems.

13. Plaintiffs bring this action individually and on behalf of the Class and seek actual damages, statutory damages, punitive damages, and restitution, with attorneys' fees, costs, and expenses, and further sue Defendants for, among other causes of action, negligence, breach of implied contract, unjust enrichment, and California and Oregon consumer statutes. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendants' data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court deems necessary and proper.

JURISDICTION AND VENUE

14. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest

and costs, Plaintiff Bulling is a citizen of the State of Oregon, and many other members of the Class are citizens of states different from Defendants.

15. The Court has personal jurisdiction over Defendants because Defendants' principal place of business is located in this District and Defendants conduct substantial business in California and this District.

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

PARTIES

17. Plaintiff Erik Solter is a citizen of the State of California and resides in Los Angeles County, California. He received notice from Defendant Tennis Warehouse on or about December 22, 2021, informing him of the Data Breach.

18. Plaintiff Lorne Bulling is a citizen of the State of Oregon and resides in Washington County, Oregon. He received notice from Defendant Tennis Warehouse on or about December 17, 2021, informing him of the Data Breach.

19. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class members; (ii) warn Plaintiffs and Class members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates numerous state and federal laws.

20. Plaintiffs and Class members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

21. Defendants obtained and continue to maintain Plaintiffs' PII and have a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiffs would not have entrusted their PII to Defendants had they known that Defendants would fail to maintain adequate data security. Plaintiffs' PII was compromised and disclosed as a result of the Data Breach.

22. As a result of the Data Breach, Plaintiffs have already spent, and anticipate spending, considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs will continue to be at increased risk of identity theft and fraud.

23. Like Plaintiffs, the other Class members have a continuing interest in ensuring that their PII is protected and safeguarded from future breaches.

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

a. unauthorized use of their PII;

b. theft of their PII;

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

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

e. time spent and costs associated with 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 researching the potential impact of the Data Breach, evaluating and enrolling in credit monitoring, purchasing

identity protection, reviewing bank account statements, credit card statements, credit reports, and online accounts, evaluating implementation of a credit freeze, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. damages arising from the theft of their PII, including addressing identity theft and fraudulent accounts and loans;

g. damages to and diminution in value of their PII entrusted to Defendants;

h. the loss of Plaintiffs' and Class members' privacy; and

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

25. Defendant Sports Warehouse d/b/a Tennis Warehouse is a California corporation with its principal place of business at 181 Suburban Road, San Luis Obispo, California, 93401. Defendant Tennis Warehouse's agent for service of process is Mark Adam Sczbecki, 181 Suburban Road, San Luis Obispo, California, 93401. Defendant Sports Warehouse operates as a sporting goods business and generates $89.46 million in annual revenue.[2] Defendant Sports Warehouse operates the website www.tennis-warehouse.com.

26. Defendant Running Warehouse, LLC is a California company with its principal place of business at 181 Suburban Road, San Luis Obispo, California, 93401. Defendant Running Warehouse's agent for service of process is Mark Sczbecki, 181 Suburban Road, San Luis Obispo, California, 93401. Defendant

[2] *See* https://www.dnb.com/business-directory/company-profiles.sports_warehouse.e03fc17750ced37157a9634b2ebd9b0a.html (last accessed January 21, 2022).

Running Warehouse operates as an online shoe, clothing and running gear business through the website runningwarehouse.com and generate $11.12 million in annual revenue.[3]

27. Defendant Wilderness Sports Warehouse LLC d/b/a Tackle Warehouse is a California company with its principal place of business at 181 Suburban Road, San Luis Obispo, California, 93401. Defendant Tackle Warehouse's agent for service of process is Mark Sczbecki, 181 Suburban Road, San Luis Obispo, California, 93401. Defendant Tackle Warehouse operates as an online fishing and sporting goods business through the website tacklewarehouse.com and generates $15.91 million in annual revenue.[4]

28. Defendant Skate Warehouse, LLC is a California company with its principal place of business at 181 Suburban Road, San Luis Obispo, California, 93401. Defendant Skate Warehouse's agent for service of process is Mark Sczbecki, 181 Suburban Road, San Luis Obispo, California, 93401. Defendant Skate Warehouse operates as an online business selling skateboards, longboards, and skate clothing and footwear through the website skatewarehouse.com and generates $1.06 million in annual revenue.[5]

29. Defendants make sizeable profits at the expense of their customers; however, Defendants betrayed the trust of their customers by putting their PII at risk

---

[3] *See* https://www.dnb.com/business-directory/company-profiles.running_warehouse_llc.b85ef65e193dcd63a641e7d6698d8e3b.html (last accessed January 21, 2022).

[4] *See* https://www.dnb.com/business-directory/company-profiles.wilderness_sports_warehouse_llc.ff2f2aa5fa8da12781f8ec955f2ca7f0.html (last accessed January 21, 2022).

[5] *See* https://www.dnb.com/business-directory/company-profiles.skate_warehouse_llc.e6159b715456b5145e4d5a5efd8e1dac.html (last accessed January 21, 2022).

of attack by cybercriminals. Defendants' actions and/or inaction exposed their customers' PII, including highly sensitive PII, to cyberattack. Through this lawsuit, the numerous affected customers who entrusted their PII to Defendants have a voice in Plaintiffs.

STATEMENT OF FACTS

I. The Data Breach

30. On October 1, 2021, Defendants' computer systems were subject to a data security incident through which threat actors gained unauthorized access to Plaintiffs' and Class members' PII, including highly sensitive payment card information.

31. Defendants discovered the Data Breach on October 15, 2021, but did not begin notifying affected individuals until on or around December 16, 2021, two and one-half (2 1/2) months after the Data Breach.

32. On or about December 16, 2021 – two (2) months after first learning of the Data Breach – Defendants began sending out Notifications of Data Security Incident to their customers whose information was accessed and exposed in the Data Breach.

33. It is apparent from the various notices and sample notices of the Data Breach sent to Plaintiffs, the Class, and state Attorneys General that the PII contained within its computer systems was not adequately secured and protected.

34. Following discovery of the Data Breach, Defendants began an internal investigation and engaged an independent computer forensics firm to address the Data Breach. Based upon the investigation, the attackers were able to access certain computer systems containing the PII at issue.

35. Upon information and belief, the unauthorized third-party cybercriminals gained access to the PII with the intent of engaging in misuse of the

PII, including marketing and selling Plaintiffs' and Class members' PII on the dark web.

36. Despite the severity of the Data Breach, Defendants have not adequately protected Plaintiffs and the Class. For example, upon information and belief, in the Notification of Data Security Incident, Defendants did not provide adequate identity theft or credit monitoring protection for the individuals affected by the Data Breach by having their payment card information exposed.

37. In effect, Defendants are shirking their responsibility for the harm and increased risk of harm they have caused Plaintiffs and members of the Class, including the distress and financial burdens the Data Breach has placed upon the shoulders of the Data Breach victims.

38. To make matters worse, Defendants' attackers gained access to, and possession of, Plaintiffs' and Class members' PII. While many data breach events merely involve the attacker gaining access to the computer or network without meaningful access to the victims' information, in this particular attack on Defendants' systems, hackers gained access to Plaintiffs' and Class members' highly sensitive PII, including financial account numbers, and credit and debit card numbers with CVVs.

39. Defendants failed to adequately safeguard Plaintiffs' and Class members' PII, allowing cyber criminals to access this sensitive financial information for over two and one-half (2 1/2) months before warning the criminals' victims to be on the lookout, and now offer them no remedy or relief.

40. Defendants failed to spend sufficient resources on cybersecurity training and adequate data security measures and protocols.

41. Plaintiffs and Class members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

42. Defendants had a duty pursuant to common law, industry standards, and payment card network rules to keep consumers' card information confidential and to protect it from unauthorized access.

43. Defendants failed to properly safeguard Class members' payment card information, allowing cybercriminals to access the credit and debit card information.

II. Plaintiff Solter's Experience

44. Plaintiff Solter purchased items from websites operated by Defendant Tennis Warehouse, specifically www.racquetballwarehouse.com for which he received confirmation from tennis-warehouse.com, prior to October 1, 2021. He used his Los Angeles Police Federal Credit Union (Police Credit Union) payment card for his purchases. He received Defendants' Notice of Data Breach, dated December 22, 2021, on or about that date.

45. In mid-December of 2021, following the Data Breach, the Police Credit Union notified Plaintiff Solter that fraudulent charges were made on his payment credit card and that the Police Credit Union would be replacing his credit card as a result. Plaintiff heavily relied on this payment card. He was without the use of his card for many days. He had his new payment card shipped to him by overnight mail at a cost in excess of $25 to gain quicker access thereto.

46. In addition, many of Plaintiff Solter's bills were connected to the compromised payment card that had to be replaced, resulting in late payments and late fees associated with said payments. Solter has incurred at least $25 in late fees associated with the compromised payment card account.

47. After receiving the Notification of Data Security Incident, Plaintiff Solter spent more than ten (10) hours dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including reviewing and monitoring his bank accounts, credit card accounts, credit reports and other online accounts, evaluating freezing his credit with credit reporting agencies

and credit protection services, and evaluating credit monitoring services and identity protection services.

48. Plaintiff Solter has suffered out-of-pocket expenses, lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy, which he would not have suffered had Defendants implemented the necessary and proper safeguards to protect their customers' PII from theft.

49. Plaintiff Solter has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

III. Plaintiff Bulling's Experience

50. Plaintiff Bulling purchased items from websites operated by Defendant Tennis Warehouse, specifically tennis-warehouse.com, prior to October 1, 2021. He used his payment card for the purchase(s). He received Defendants' Notice of Data Security Incident, dated December 17, 2021, on or about that date.

51. After receiving the Notice of Data Security Incident, Plaintiff Bulling canceled the payment card he had used at tennis-warehouse.com and requested a replacement as a result of the Data Breach. In addition, Bulling implemented a freeze on his credit with Equifax.

52. After receiving the Notice of Data Security Incident, Plaintiff Bulling spent more than five (5) hours dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including reviewing and monitoring his bank accounts, credit card accounts, credit reports and other online accounts, researching the potential impact of the Data Breach, freezing his credit with credit reporting agencies and credit protection services, including TransUnion, and evaluating credit monitoring services and identity protection services.

53. Plaintiff Bulling has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy, which he would not have suffered had Defendants implemented the necessary and proper safeguards to protect their customers' PII from theft.

54. Plaintiff Bulling has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

IV. Defendants Had a Duty to Safeguard the PII Within Their Possession

55. Defendants are required to protect Plaintiffs' and Class members' PII, and further, to handle any data breach of the same in accordance with applicable federal and state law.

56. In addition to their obligations under federal and state law, Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII of the Class.

57. Defendants owed a duty to Plaintiffs and the Class to design, maintain, and test their computer systems and networks to ensure that the PII in Defendants' possession was adequately secured and protected.

58. Defendants owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the PII in their possession.

59. Defendants owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on their data security systems in a timely manner.

60. Defendants owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

61. Defendants owed a duty to Plaintiffs and the Class to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII with Defendants.

62. Defendants owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

63. Defendants owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate data security practices.

64. Plaintiffs and other Class members relied on Defendants to implement and maintain systems that kept their PII safe. Defendants had a duty to keep their customers' PII safe, particularly given the highly sensitive nature of the information stored on Defendants' computer systems. Defendants failed to comply with all of these foregoing duties.

V. Defendants Were Well Aware of Their Data Security Obligations Given the Increase in Payment Card Data Breaches

65. Defendants were well aware of their data security obligations given the substantial increase in payment card data breaches throughout the retail industry preceding the Data Breach. The increase in data breaches and the risk of future breaches were widely known throughout the retail industry, including to Defendants. For instance, Experian reported that 14.2 million Americans had their credit card numbers stolen in 2017, an 88% increase in the amount of credit cards numbers stolen in the United States from 2016.

66. Furthermore, Defendants' data security obligations and promises were particularly important given the many high-profile payment card data breaches that have been reported in recent years, which were widely known to the public and to any entity, like Defendants, that conducts a substantial amount of business via payment cards. In recent years, massive payment card data breaches have impacted large retailers and restaurants, including Arby's, Chipotle, Dairy Queen, Forever 21, GameStop, Harbor Freight Tools, Home Depot, Hy-Vee, Kmart, Lord & Taylor, Michael's Stores, Neiman Marcus, Noodles & Co., P.F. Chang's, Saks Fifth Avenue, Sally Beauty Supply, Schnuck Markets, SuperValu, Target, T.J. Maxx, Wendy's, and many others. Large breaches have impacted not just retailers and restaurants, but also large companies responsible for housing important and sensitive consumer financial and medical data. The high-profile breaches that impacted Marriott, Equifax, Yahoo, Premera, and Anthem serve as additional examples of the consequences of inadequate data security, and these breaches put Defendants on further notice of the need to have robust data security protections in place.

67. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have "engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data," including recent cases against Uber Technologies, Venmo, and VTech Electronics.[6] The FTC has publicized these and other enforcement actions so that companies entrusted with sensitive financial information are aware of their duty and can improve their practices for safeguarding customer information.[7]

---

[6] Fed. Trade Comm'n, *Privacy & Data Security* (2018), at p.5, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf (last accessed January 21, 2022).

[7] *See* Fed. Trade Comm'n, *Start With Security: A Guide For Business, Lessons*

(footnote continued)

VI. Cyber Criminals Will Use Plaintiffs' and Class Members PII for Nefarious Purposes

68. Plaintiffs' and Class members' highly sensitive PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiffs and the Class members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access Defendants' systems in order to obtain valuable PII to sell on the dark web.

69. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[8] These criminal activities have resulted and will result in devastating financial and personal losses to Plaintiffs and Class members.

70. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

71. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[9]

Learned From FTC Cases (2015), at p. 1, https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf (last accessed January 21, 2022).

[8] *See Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last accessed on January 21, 2022).

[9] *See* Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-willidentity-thieves-use-stolen-info (last accessed January 21, 2022).

72. Hackers might not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[10]

73. If cyber criminals manage to access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may expose the Plaintiffs and Class members and that fraud can occur for years following the Data Breach, thereby exposing Plaintiffs and Class members to years of risk and the need to carefully monitor all of their financial data and accounts every month.

VII. Defendants Violated the Payment Card Industry Data Security Standard

74. There is an extensive network of financial institutions, card-issuing banks, and card-processing companies involved in credit and debit card transactions. Card networks have issued detailed rules and standards governing the basic protective measures that merchants like Defendants must take to ensure that payment card information is properly safeguarded.

75. Furthermore, the payment card networks (primarily MasterCard, Visa, American Express, and Discover) have issued card operating rules that are binding

---

[10] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archiveit.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolenlaptops-lead-to-important-hipaa-settlements.html (last accessed January 21, 2022).

on merchants, including Defendants, and require merchants to protect payment card information. In particular, the Payment Card Industry Security Standards Council promulgates minimum standards that apply to all organizations that store, process, or transmit payment card data, known as PCI DSS. PCI DSS is the universal industry standard governing the security of credit and debit card data.

76. PCI DSS establishes detailed and comprehensive requirements for satisfying each of the following twelve "high-level" mandates:[11]

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

77. PCI DSS sets the minimum level of what must be done to protect the cardholder data environment ("CDE"). While PCI DSS compliance is an important first step in securing cardholder data such as the payment card information compromised in the Data Breach, it is not sufficient on its own to protect against

[11] *Payment Card Industry (PCI) Data Security Standard*, PCI SECURITY STANDARDS COUNCIL (May 2018), at p. 5, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-21.pdf?agreement=true&time=1577046042482 (last accessed January 21, 2022).

compromises that may in turn breach the CDE, nor does it provide a safe harbor against civil liability for a data breach.

78. Defendants violated numerous provisions of PCI DSS, including subsections underlying the high-level mandates in the chart above. Those deficiencies will be revealed during discovery.

79. Industry experts acknowledge that a data breach is indicative of data security failures. For example, research and advisory firm Aite Group has stated: "'If your data was stolen through a data breach that means you were somewhere out of compliance' with payment industry data security standards."[12]

80. Defendants were active participants in the payment card networks as they collected and transmitted numerous sets of payment card data per day. At all relevant times, Defendants knew of their PCI DSS obligations to protect cardholder data such as the payment card information compromised in the Data Breach, but Defendants failed to uphold their data security obligations.

VIII. Damages Sustained by Plaintiffs and Class Members

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

a. unauthorized use of their PII;

b. damages arising from the inability to use their PII;

c. monetary costs associated with their attempts to ameliorate, mitigate and deal with the actual and future consequences of the breach, including the freezing of their credit, and enrolling in credit or identity monitoring services;

---

[12] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017, 2:29 PM), https://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last accessed January 21, 2022).

d. time spent and monetary and other costs associated with the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiffs and Class members could have been working and earning a living, therefore suffering further actual injury);

e. the imminent and impending injury flowing from actual and potential fraud and identity theft posed by their PII being placed in the hands of criminals;

f. damages to and diminution in value of their PII entrusted to Defendants for the sole purpose of purchasing products and services from websites operated by Defendants; and

g. the loss of Plaintiffs' and Class members' privacy.

CLASS ACTION ALLEGATIONS

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

> **All natural persons residing in the United States of America whose PII was compromised in the Data Breach that occurred in October 2021 (the "Nationwide Class" or "Class"), including all United States residents who were sent a notice of the Data Breach.**

83. In addition, Plaintiff Bulling brings this action on behalf of himself and on behalf of a subclass defined as:

> **All natural persons residing in the State of Oregon whose PII was compromised in the Data Breach that occurred in October 2021 (the "Oregon Subclass"), including all United States residents who were sent a notice of the Data Breach.**

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

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

86. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number at least in the tens of thousands and likely more.

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

a. Whether Defendants failed to use reasonable care and reasonable methods to secure and safeguard Plaintiffs' and Class members' PII;

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

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

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

e. Whether Defendants failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' PII;

f. Whether Defendants were negligent in failing to properly secure and protect Plaintiffs' and Class members' PII; and

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

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

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

90. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives 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' interests will be fairly and adequately protected by Plaintiffs and their counsel.

91. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted and/or refused to act on grounds that apply generally to the

Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

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

FIRST CLAIM FOR RELIEF
Negligence
(***On Behalf of Plaintiffs and the Nationwide Class***)

93. Plaintiffs, individually and on behalf of the Class, repeat and re-allege the allegations contained in paragraphs 1 through 92 as though fully set forth herein.

94. By virtue of their express undertaking to protect Class members' PII and upon accepting and storing Plaintiffs' and Class members' PII, Defendants undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use reasonable methods to do so. Defendants knew that the PII was confidential and should be protected as private and confidential.

95. Defendants owed a duty of care not to subject Plaintiffs' and Class

members' PII to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

96. Defendants owed numerous duties to their customers, Plaintiffs and Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches on their own systems and those of their third parties.

97. Defendants failed to provide adequate supervision and oversight of the PII with which they were, and are, entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' PII, misuse the PII and intentionally disclose it to others without consent.

98. Defendants knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of their data collection and/or storage systems, and the importance of adequate security.

99. Defendants knew, or should have known, that their data collection and/or storage systems and networks, including their third-party affiliates, did not adequately safeguard Plaintiffs' and Class members' PII.

100. Defendants breached their duties to Plaintiffs and Class members by failing to ensure that their agents and affiliates were providing fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

101. Because Defendants knew that a breach of their systems would damage an untold number of their customers, including Plaintiffs and Class members, Defendants had a duty to adequately safeguard their data systems and the PII contained thereon. Moreover, only Defendants had the ability to protect their systems and those of their affiliates, and the PII they stored on them, from attack.

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

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

104. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII to Plaintiffs and the Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII. Defendants failed to do so, only disclosing the Data Breach two and a half (2 1/2) months after it occurred.

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

106. Upon information and belief, neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

107. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer damages and injury, including but not limited to:

a. unauthorized use of their PII;

b. theft of their PII;

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

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

e. time spent and monetary and other costs associated with 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, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiffs and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from their PII being placed in the hands of criminals;

g. damages to and diminution in value of their PII entrusted to Defendants for the sole purpose of purchasing products and services from website operated by Defendants; and

h. the loss of Plaintiffs' and Class members' privacy.

108. As a direct and proximate cause of Defendants' negligence, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury

and/or harm, including, but not limited to loss of privacy, and other economic and non- economic losses.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(*On Behalf of Plaintiffs and the Nationwide Class*)

109. Plaintiffs, individually and on behalf of the Nationwide Class, repeat and re-allege the allegations contained in paragraphs 1 through 92 as though fully set forth herein.

110. When Plaintiffs and Class members provided their PII, including payment card information, to Defendants in exchange for Defendants' products, they entered into implied contracts with Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect the payment card information and other PII.

111. Defendants solicited and invited Plaintiffs and Class members to provide their payment card information as part of Defendants' regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts between Plaintiffs and Class members on one hand, and Defendants on the other hand. Plaintiffs and Class members accepted Defendants' offers by providing their payment card information to Defendants in connection with purchases at Defendants.

112. Plaintiffs and the Nationwide Class provided their personal and financial information to Defendants in the course of purchasing products from Defendants. In so doing, Plaintiffs and the Nationwide Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

113. When entering into the implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

114. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendants.

115. Defendants breached the implied contracts they made with Plaintiffs and the Nationwide Class by failing to safeguard and protect their personal and financial information, and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

116. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic harm.

THIRD CLAIM FOR RELIEF
Unjust Enrichment
(*On Behalf of Plaintiffs and the Nationwide Class*)

117. Plaintiffs, individually and on behalf of the Class, repeat and re-allege the allegations contained in paragraphs 1 through 92 as though fully set forth herein.

118. By engaging in the conduct described in this Complaint, Defendants have knowingly obtained benefits from Plaintiffs and the Class, and actual monies

and other benefits under circumstances such that it would be inequitable and unjust for these Defendants to retain them.

119. By engaging in the acts and failures to act described in this Complaint, Defendants have been knowingly enriched by the savings in costs that should have been reasonably expended to protect the PII of Plaintiffs and the Class. Defendants knew or should have known that theft of customer PII could happen, yet they failed to take reasonable steps to pay for the level of security required to have prevented the theft of their customers' PII.

120. By engaging in the conduct described in this Complaint, Defendants have knowingly obtained benefits from Plaintiffs and the Class under circumstances such that it would be inequitable and unjust for Defendants to retain them.

121. Defendants will be unjustly enriched if they are permitted to retain the benefits derived from the theft of Plaintiffs' and the Class' PII.

122. Plaintiffs and each member of the Class are therefore entitled to an award of compensatory damages in an amount to be determined at trial, or the imposition of a constructive trust upon the monies derived by Defendants by means of the above-described actions.

FOURTH CLAIM FOR RELIEF
Violations of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100, *et seq.*
(*On Behalf of Plaintiff Solter and the Nationwide Class*)

123. Plaintiff Solter, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 92 as though fully set forth herein.

124. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security

procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

125. Plaintiff Solter is a "consumer" as defined by Civ. Code § 1798.140(g) because he is a "natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

126. Defendants are "business[es]" as defined by Civ. Code § 1798.140(c) because each:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners;"

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information;"

c. does business in and is headquartered in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

127. Plaintiff Solter's PII was subject to unauthorized access and exfiltration, theft or disclosure because of Defendants' inadequate security measures.

128. Plaintiff Solter's PII was in nonencrypted and nonredacted form, allowing criminals full access to it.

129. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. Defendants failed to implement reasonable security procedures to prevent unauthorized access of Plaintiff Solter's and Class members' PII as a result of a cyber-attack.

130. Plaintiff Solter sent a written notice to Defendants pursuant to Civil Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have or are violating. Although a cure is not possible under the circumstances, if as expected Defendants are unable to cure or do not cure the violation within 30 days, Plaintiff will amend this complaint to pursue actual or statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

131. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff Solter seeks actual damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

FIFTH CLAIM FOR RELIEF
Violations of the California Unfair Competition Law
Cal. Civ. Code §§ 17200, *et seq.*
(*On Behalf of Plaintiffs and the Nationwide Class*)

132. Plaintiffs, individually and on behalf of the Class, repeat and re-allege the allegations contained in paragraphs 1 through 92 as though fully set forth herein.

133. The California Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq.*, prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

134. In the course of conducting their business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, the CCPA, Section 5 of the FTCA and Article I, Section 1 of the California Constitution, California's constitutional right to privacy. Plaintiff and Class members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

135. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends legislatively declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution (California's constitutional right to privacy), and Section 5 of the FTCA. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

136. The UCL also prohibits any "fraudulent business act or practice." Defendants' inadequate data security practices as described herein were fraudulent, misleading and likely to deceive the consuming public in violation of the UCL.

137. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' violations of the UCL. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

138. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct, and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to them, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

SIXTH CLAIM FOR RELIEF
Oregon Consumer Identity Theft Protection Act,
Or. Rev. Stat. §§ 646A.604(1), *et seq.*
(*On Behalf of Plaintiff Bulling and the Oregon Subclass*)

139. Plaintiff Bulling, individually and on behalf of the Oregon Subclass, repeats and re-alleges the allegations contained in paragraphs 1 through 92 as though fully set forth herein.

140. Defendants are businesses that maintain records which contain PII, within the meaning of Or. Rev. Stat. § 646A.622(1), about Plaintiff Bulling and Oregon Subclass members.

141. Pursuant to Or. Rev. Stat. § 646A.622(1), a business "that maintains records which contain Personal Information" of an Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

142. Defendants violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff Bulling's and Oregon Subclass members' PII.

143. Defendants are businesses that own, maintain, or otherwise possess data that includes consumers' Personal Information as defined by Or. Rev. Stat. § 646A.604(1).

144. Plaintiff Bulling's and Oregon Subclass members' PII includes Personal Information as covered under Or. Rev. Stat. § 646A.604(1).

145. Defendants are required to accurately notify Plaintiff Bulling and Oregon Subclass members if they become aware of a breach of their data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. § 646A.604(1).

146. Because Defendants discovered a breach of their security systems, they had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Or. Rev. Stat. § 646A.604(1).

147. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Or. Rev. Stat. § 646A.604(1).

148. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

149. As a direct and proximate result of Defendants' violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff Bulling and Oregon Subclass members suffered damages, as described above.

150. Plaintiff Bulling and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

SEVENTH CLAIM FOR RELIEF
Oregon Unlawful Trade Practices Act,
Or. Rev. Stat. §§ 646.608, *et seq.*
(*On Behalf of Plaintiff Bulling and the Oregon Subclass*)

151. Plaintiff Bulling, individually and on behalf of the Oregon Subclass, repeats and re-alleges the allegations contained in paragraphs 1 through 92 as though fully set forth herein.

152. Defendants are "person[s]," as defined by Or. Rev. Stat. § 646.605(4).

153. Defendants engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

154. Defendants advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

155. Defendants engaged in unlawful practices in the course of their business and occupation, in violation of Or. Rev. Stat. § 646.608, including the following:

a. Representing that their goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Representing that their goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertising their goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and

d. Concurrent with tender or delivery of their goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

156. Defendants' unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Bulling's and Oregon Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bulling's and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Bulling's and Oregon Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and

statutory duties pertaining to the security and privacy of Plaintiff Bulling's and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Bulling's and Oregon Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bulling's and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*

157. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

158. Defendants intended to mislead Plaintiff Bulling and Oregon Subclass members and induce them to rely on Defendants' misrepresentations and omissions.

159. Had Defendants disclosed to Plaintiff Bulling and Oregon Subclass members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

160. Defendants acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff Bulling's and Oregon Subclass members' rights.

161. As a direct and proximate result of Defendants' unlawful practices, Plaintiff Bulling and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

162. Plaintiff Bulling and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the members of the Classes, respectfully requests the Court to enter an Order:

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

B. Ordering Defendants to pay actual/statutory damages as appropriate to Plaintiffs and the other members of the Class;

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands a trial by jury on all claims so triable.

Date: January 21, 2022

Respectfully submitted,

/s/ Benjamin Heikali

FARUQI & FARUQI, LLP
Benjamin Heikali (State Bar No. 307466)
bheikali@faruqilaw.com
Ruhandy Glezakos (SBN 307473)
Email: *rglezakos@faruqilaw.com*
Joshua Nassir (State Bar No. 318344)
Email: *jnassir@faruqilaw.com*
10866 Wilshire Boulevard, Suite 1470
Los Angeles, California 90024
Telephone: (424) 256-2884
Facsimile: (424) 256-2885

GEORGE GESTEN MCDONALD, PLLC
Lori G. Feldman*
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
Fax: (888) 421-4173
Email: *LFeldman@4-Justice.com*
E-Service: *eService@4-Justice.com*

GEORGE GESTEN MCDONALD, PLLC

David J. George*
Brittany L. Brown*
9897 Lake Worth Road, Suite #302
Lake Worth, Florida 33467
Telephone: (561) 232-6002
Fax: (888) 421-4173
Email: *DGeorge@4-Justice.com*
BBrown@4-Justice.com
E-Service: *eService@4-Justice.com*

CALCATERRA POLLACK, LLP
Janine L. Pollack*
Michael Liskow (Cal Bar No. 243899)
1140 Avenue of the Americas
9th Floor
New York, New York 10036
Telephone: (917) 899-1765
Fax: (332) 206-2073
Email: *jpollack@calcaterrapollack.com*
mliskow@calcaterrapollack.com

Attorneys for Plaintiffs

**Pro hac vice forthcoming*