William B. Federman (*pro hac vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560 (telephone)
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

Co-Interim Class Counsel for the Plaintiffs and Putative Class

[additional counsel listed on signature block]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN RE SNAP FINANCE DATA BREACH LITIGATION This Document Relates to:	Lead Case No. 2:22-cv-00761-TS-JCB **PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

Plaintiffs Tracy Tanner, Victor Sanchez, Tameka Montgomery, Sterling Simeon, Monique Grayes, Carolyn Saunders, Nick Peppelaar, and Tara Schulmeister ("Plaintiffs"), individually and on behalf of all others similarly situated, through Counsel, and for the Consolidated Class Action Complaint for Damages against Defendants Snap Finance LLC ("SF") and Snap RTO LLC ("SP") (collectively, "Defendants"), and alleges upon personal knowledge as to their own actions and experiences, and upon investigation, information, and belief as to all other matters, as follows:

INTRODUCTION

1. This consumer data breach lawsuit arises out of Defendants' failure to implement and maintain adequate security and safeguards with respect to the collection and maintenance of highly sensitive and confidential personal information of their customers, including Plaintiffs' and Class members' names, Social Security numbers, driver's license numbers, state identification

numbers, and financial account numbers. Defendants' insufficient and unreasonable data security practices caused, facilitated, and exacerbated the data breach and its impact on Plaintiffs and Class members.

2. Defendant Snap Finance LLC is a Utah limited liability company based in South West Valley, Utah, and Defendant Snap RTO LLC is a Utah limited liability company based in Salt Lake City, Utah. The two entities refer to themselves collectively as "Snap."[1]

3. Defendants are in the financial services industry, they are in the "lease to own" lending business with "fast" loans, which can range as high as $5,000 dollars.[2]

4. On December 1, 2022, Defendants sent to Plaintiffs and Class members a letter entitled "Notice of Security Incident" ("Notice"). The Notice stated that, between June 23, 2022 and September 8, 2022, an unauthorized actor had the ability to access certain information stored on Defendants' network (the "Data Breach"). According to Defendants, on or about October 28, 2022, Defendants determined through their ongoing investigation that personal information of their customers was affected. Although Defendants identified suspicious activity much earlier, Defendants did not warn those most at risk—Plaintiffs and Class members—until December 1, 2022.

5. The Data Breach exposed Plaintiffs' and Class members' personally identifiable information to criminals, including, but not limited to, their names, Social Security numbers, driver's license numbers, state identification numbers, and financial account numbers. Because Defendants hold loans and collateral on those loans, Plaintiffs and Class members reasonably

[1] Office of Maine Attorney General, Data Breach Notifications, (Dec. 2, 2022), https://apps.web.maine.gov/online/aeviewer/ME/40/d193f4eb-a877-4395-9a3c-8b94833c907c.shtml (last visited Feb. 4, 2023).
[2] Snap, https://snapfinance.com/how-it-works, (last visited on Feb. 4, 2023).

believe additional information concerning their finances, personal accounts, credit files, and property information, as well as all other types of information concerning themselves and their loans obtained by Defendants, are also exposed. All of the foregoing information pertaining to Plaintiffs and Class members is referred to herein as "PII."

6. The PII that Defendants failed to protect with reasonable safeguards can be used by criminals alone, and in conjunction with other pieces of information, to perpetrate crimes against Plaintiffs and Class members that can result in significant liability and damage to their money, property, creditworthiness, reputation, and their ability to prove their identity, pay current loans, improve their credit, and/or obtain loans on favorable terms in the future.

7. Plaintiffs and Class members entrusted Defendants with their PII. Defendants understand the importance of protecting such information. For example, on one of Defendants' websites, it states: "How Snap protects your information" and explains that "Snap stores and processes your information maintaining physical, electronic and procedural safeguards. We maintain physical security measures to guard against unauthorized access to systems and use safeguards such as firewalls and data encryption. We enforce physical access controls to our buildings, and we authorize access to personal information only for those employees or contractors who require it to fulfill the responsibilities of their jobs."[3]

8. Defendants' representations concerning privacy practices and data security were false. Defendants do not state the date they began investigating the incident, only that on or around October 28, 2022, Defendants completed their review and determined that their customers' information was accessed in the Data Breach that occurred between June 23, 2022 and September 8, 2022. Criminals breached Defendants' inadequately defended systems, and accessed and

[3] *See* https://snapfinance.com/legal/privacy. (last visited Feb. 4, 2023).

acquired electronic files containing the PII of Plaintiffs and Class members. The criminals gained unauthorized access by thwarting, circumventing, and defeating Defendants' unreasonably deficient data security measures and protocols. Defendants did not start notifying Plaintiffs and Class members of the Data Breach until on or around December 1, 2022.

9. Plaintiffs, individually, and on behalf of all persons similarly situated, seek to be made whole for the losses incurred as a result of the Data Breach, and the losses that will be incurred in the future. Plaintiffs also seeks injunctive relief in the form of compliant data security practices, full disclosure regarding the disposition of the information in Defendants' systems, and monitoring and audits of Defendants' security practices going forward because Defendants continue to collect, maintain, and store Plaintiffs' and Class members' PII. Due to the sensitive and immutable nature of the PII at issue, especially Social Security numbers, Plaintiffs and Class members will need to, among other things, enroll is identity theft protective services for their respective lifetimes.

PARTIES, JURISDICTION, AND VENUE

10. Plaintiff Tracy Tanner ("Plaintiff Tanner") is a resident and citizen of the State of Ohio. Plaintiff Tanner received a letter from Snap, notifying him that his PII, including his Social Security number and driver's license number, had been compromised in the Data Breach.

11. Plaintiff Victor Sanchez ("Plaintiff Sanchez") is a resident and citizen of the State of Nevada. Plaintiff Sanchez received a letter from Snap, notifying him that his PII, including his Social Security number and driver's license number, had been compromised in the Data Breach.

12. Plaintiff Tameka Montgomery ("Plaintiff Montgomery") is a resident and citizen of the State of Illinois. Plaintiff Montgomery received a letter from Snap, notifying her that his

PII, including her Social Security number and driver's license number, had been compromised in the Data Breach.

13. Plaintiff Sterling Simeon ("Plaintiff Simeon") is a resident and citizen of the State of California. Plaintiff Simeon received a letter from Snap, notifying him that his PII, including his Social Security number and driver's license number, had been compromised in the Data Breach.

14. Plaintiff Monique Grayes ("Plaintiff Grayes") is a resident and citizen of the State of California. Plaintiff Grayes received a letter from Snap, notifying her that her PII, including her Social Security number and driver's license number, had been compromised in the Data Breach.

15. Plaintiff Carolyn Saunders ("Plaintiff Saunders") is a resident and citizen of the State of California. Plaintiff Saunders received a letter from Snap, notifying her that her PII, including her Social Security number and driver's license number, had been compromised in the Data Breach.

16. Plaintiff Nick Peppelaar ("Plaintiff Peppelaar") is a resident and citizen of the State of Utah. Plaintiff Peppelaar received a letter from Snap, notifying him that his PII, including his Social Security number and driver's license number, had been compromised in the Data Breach.

17. Plaintiff Tara Schulmeister ("Plaintiff Schulmeister") is a resident and citizen of the State of Ohio. Plaintiff Schulmeister received a letter from Snap, notifying her that her PII, including her Social Security number and driver's license number, had been compromised in the Data Breach.

18. Defendant Snap Finance LLC is a Utah limited liability company with its principal place of business in South West Valley, Utah.

19. Defendant SNAP RTO LLC is a Utah limited liability company with its principal place of business in South Salt Lake City, Utah.

20. The Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action involving 100 or more Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Many members of the Class, including Plaintiffs, are citizens of different states from Defendants.

21. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2), as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conducts substantial business in this District.

22. All of Plaintiffs' and Class Members' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns. As the corporate relationship between the two Defendants and other possible defendants is not fully known, Plaintiffs and Class Members reserve the right to amend the complaint should the facts and the evidence necessitate it.

GENERAL ALLEGATIONS

Background

23. For Snap to perform their financing services, from which they generate their profits, Defendants collect and store the PII of individuals, including Plaintiffs and the Class.

24. Snap is in the business of providing "lease to own financing" for consumer items as well as other kinds of loans and extensions of credit.[4] Snap touts its ability to allow customers to purchase items quickly, and to "pay over time." It allows people to purchase items over time and make payments.

[4] Snap, How it Works, https://snapfinance.com/how-it-works (last visited on Feb. 4, 2022).

25. Snap uses a network of over 150 retailers whereby Snap customers can use Snap's loans and loan payment structures to pay for goods and services over time.[5] Snap claims it allows customers to pay the loan when they receive their paycheck, which, for all intents and purposes makes it a "payday lender." On information and belief, in the ordinary course of business, Defendants collect sensitive personal and private information from their customers such as:

- Demographic information (i.e., first and last name, home address, phone number, email address, and date of birth);
- Social Security numbers;
- Driver's License or state identification numbers; and
- Financial information.

26. Due to the highly sensitive and personal nature of the information Defendants acquires and stores with respect to loan applicants and customers, Defendants recognizes the privacy rights of the individuals whose PII Defendants obtains, as evidenced by Snap's publicly available privacy policy ("Privacy Notice").[6] Defendants' Privacy Notice promises to, among other things, that:

> Snap stores and processes your information maintaining physical, electronic and procedural safeguards. We maintain physical security measures to guard against unauthorized access to systems and use safeguards such as firewalls and data encryption. We enforce physical access controls to our buildings, and we authorize access to personal information only for those employees or contractors who require it to fulfill the responsibilities of their jobs.

27. Plaintiffs and the Class Members reasonably expected that Defendants would implement and maintain reasonable data security measures to protect their PII from foreseeable threats.

---

[5] *Id.*

[6] https://snapfinance.com/legal/privacy (last visited Feb. 4, 2023).

28. Plaintiffs and Class Members relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their sensitive PII.

29. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

30. According to Defendants, "earlier this year" Defendants discovered suspicious activity in their computer "environment." Upon investigation, Defendants discovered that between June 23, 2022 and September 8, 2022 unauthorized third parties accessed their computer "environment." On or about October 28, 2022, Defendants concluded their investigation and determined that the data accessed contained the PII of Plaintiffs and Class Members. Although Defendants identified suspicious activity much earlier, and had completed their investigation by October 28, 2022 such that they knew which information and of whom was impacted, Defendants did not warn those most at risk—Plaintiffs and Class Members—until December 1, 2022.[7]

31. On December 1, 2022, Defendants transmitted to Plaintiffs and Class Members the Notice letter informing them of the Data Breach, in which their PII was compromised. The Notice stated that, between June 23, 2022 and September 8, 2022, an unauthorized actor accessed certain information (their PII) stored on Defendants' network through cyber-attack or "hacking" incident. This means that not only did the cybercriminals view and access the PII without authorization, but they also removed Plaintiffs' and Class Members' PII. In the Data Breach, these criminals acquired

[7] Office of Maine Attorney General, Data Breach Notifications, (Dec. 2, 2022), https://apps.web.maine.gov/online/aeviewer/ME/40/d193f4eb-a877-4395-9a3c-8b94833c907c.shtml (last visited Feb. 4, 2023).

the most damaging kind of PII to be exposed to unauthorized third parties: Social Security numbers, Driver's License and State identification numbers, and financial information.

32. The Notice states that Plaintiffs' and Class members' PII was accessed by an unauthorized person in the Data Breach.

33. The Notice states that Plaintiffs' and Class members' PII accessed in the Data Breach includes their names, Social Security numbers, driver's license numbers, state identification numbers, and financial account numbers.

34. The Notice does not state when the Data Breach was first detected.

35. The Notice states that "on October 28, 2022, Snap completed this review and determined the data [accessed in the Data Breach] contained certain information related to you." Defendants did not publicly announce the Data Breach, or notify those whose PII was accessed by criminals at the time they completed their "review" of the scope and extent of the Data Breach.

36. Due to Defendants' inadequate and insufficient data security measures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft and must live with that threat forever. Plaintiffs believe their PII was both stolen in the Data Breach and is still in the hands of the cybercriminal "hackers." Plaintiffs further believe their PII was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals who perpetrate cyberattacks of the type that occurred here.

Industry Standards for Data Security

37. Defendants are aware of the importance of safeguarding Plaintiffs' and Class members' PII, that by virtue of their business, they owe duties to Plaintiffs and Class members to take reasonable measures to safeguard PII that foreseeably is targeted by criminals.

38. Defendants are aware that the PII that they collect, organize, and store, can be used by criminals to engage in crimes such as identity fraud and theft using Plaintiffs' and Class members' PII.

39. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial industry preceding the date of the breach.

40. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[8]

41. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . Many of them were caused by flaws in . . . systems either online or in stores."[9]

42. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Snap knew or should have known that their electronic records would be targeted by cybercriminals.

---

[8] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at: https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/), at 6 (last visited on Feb. 4, 2023).

[9] Dennis Green, Mary Hanbury & Aine Cain, If you bought anything from these 19 companies recently, your data may have been stolen, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited Feb. 4, 2023).

43. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the Defendant's industry, including Defendants.

44. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities…are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

45. Moreover, PII is a valuable property right.[11] "Firms are now able to attain significant within the existing legal and regulatory frameworks."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

46. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other

[10] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), available at: https://www.law360.com/articles/1220974/fbi- secret-service-warn-of-targeted-ransomware (last visited Feb. , 2023).

[11] *See* Marc van Lieshout, The Value of Personal Data, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data. (last visited Feb. 4, 2023).

[12] OECD, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Feb. 4, 2023).

[13] IAB Data Center of Excellence, U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Feb. 4, 2023).

sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

47. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.[14]

48. Because of Defendants' failure to implement, maintain, and comply with necessary cybersecurity requirements, Defendants were unable to protect Plaintiffs' and Class members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality. As a proximate result of such failures, criminals gained unauthorized access to Defendants' systems, and acquired Plaintiffs' and Class members' PII in the Data Breach without being stopped.

49. Defendants were unable to prevent the Data Breach, and were unable to detect the unauthorized access to vast quantities of sensitive and protected files containing protected information of Plaintiffs and Class members. Discovery on Defendants, law enforcement investigators, and private investigators, will reveal more specific facts about Defendants' deficient and unreasonable security procedures.

[14] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1 (last visited Feb. 4, 2023).

50. Security standards commonly accepted among businesses that store personal information using the Internet include, without limitation:

a) Maintaining a secure firewall configuration;

b) Monitoring for suspicious or irregular traffic to servers;

c) Monitoring for suspicious credentials used to access servers;

d) Monitoring for suspicious or irregular activity by known users;

e) Monitoring for suspicious or unknown users;

f) Monitoring for suspicious or irregular server requests;

g) Monitoring for server requests for personal information;

h) Monitoring for server requests from VPNs; and

i) Monitoring for server requests from Tor exit nodes.

51. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[15] and protection of personal information[16] which includes basic security standards applicable to all types of businesses.

52. The FTC recommends that businesses:

a) Identify all connections to the computers where you store sensitive information;

b) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c) Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

[15] *See* F.T.C., *Start with Security: A Guide for Business*, (June 2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last accessed Feb. 8, 2023).

[16] *See* F.T.C., *Protecting Personal Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Feb. 8, 2023).

d) Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e) Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f) Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC

Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[17]

54. Because Defendants were entrusted with consumers' PII, they have a duty to keep the PII secure.

55. Plaintiffs and Class members reasonably expect that when they provide their PII to a company, the company will take reasonable measures to safeguard their PII from foreseeable cyberattacks.

56. Despite Defendants' obligations, Defendants failed to upgrade and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

57. Specifically, in breach of their duties, Defendants failed to:

a) Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;

b) Block all inbound and outbound Internet, email, and network traffic to foreign countries;

c) Maintain a secure firewall configuration;

d) Monitor for suspicious or irregular traffic to servers;

e) Monitor for suspicious credentials used to access servers;

f) Monitor for suspicious or irregular activity by known users;

g) Monitor for suspicious or unknown users;

h) Monitor for suspicious or irregular server requests;

i) Monitor for server requests for personal and financial information;

j) Monitor for server requests from VPNs;

[17] F.T.C., *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

k) Monitor for server requests from Tor exit nodes;

l) Identify all connections to the computers where Defendants store sensitive information;

m) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

n) Scan computers on Defendants' network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;

o) Pay particular attention to the security of Defendants' web applications—the software used to give information to visitors to their websites and to retrieve information from them;

p) Use a firewall to protect Defendants' computers from hacker attacks while they are connected to a network, especially the Internet;

q) Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

r) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

s) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

t) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

58. Had Defendants properly maintained their systems and adequately protected them, Defendants could have prevented the Data Breach.

Defendants Owed Duties to Plaintiffs and Class Members to Adequately Secure and Safeguard Their PII

59. Defendants are aware of the importance of security in maintaining personal information (particularly sensitive personal information), and the value consumers place on keeping their PII secure.

60. Defendants owe duties to Plaintiffs and Class members to maintain adequate security and safeguards to protect the confidentiality of their PII.

61. Defendants owe further duties to customers to immediately and accurately notify them of a breach of their systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The Categories of PII at Issue Here Are Valuable to Criminals

62. Businesses that solicit, aggregate, and store sensitive PII are likely to be targeted by cyber criminals.

63. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

64. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

65. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to a U.S. Government Accountability Office report:

> [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.[18]

66. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post PII on a number of Internet websites. Plaintiffs' and Class members' personal data that was stolen has a high value on both legitimate and black markets.

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

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[19]

68. Individuals rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy—and the amount is considerable.

69. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information—the very injury at issue here—between $11.33 and $16.58 per website.[20] The study also determined that "[a]mong U.S. subjects,

---

[18] *See* https://www.gao.gov/assets/gao-07-737.pdf at 29 (last accessed Feb. 4, 2023).

[19] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, transcript, p. 8, *available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last accessed Feb. 4, 2023).

[20] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at p. 17, Oct. 2002, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last accessed Feb. 8, 2023).

protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[21] This study was done in 2002. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

70. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

71. To date, Defendants have only offered Plaintiffs and Class members 12 months of identity theft protection. However, this is insufficient considering the fact that Plaintiffs' and Class members' PII will be used by identity thieves for many years to come.

72. The information Defendants allowed to be compromised and taken is of such that the harms to Plaintiffs and the Class will continue to grow, and Plaintiffs and Class members will continue to be at substantial risk for further imminent and future harm.

Damages from Data Breaches

73. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

74. Consumers place a high value not only on their personal information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

[21] *Id.*

75. The United States Government Accountability Office explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1024 (9th Cir. 2018). The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

76. The FTC recommends that identity theft victims take several steps to protect their personal information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports often, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

77. Identity thieves use stolen personal information for "various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud." *In re Zappos.com, Inc.*, 888 F.3d at 1024. The information exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are ways for hackers to exploit information they already have to get even more personally identifying information through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

78. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal information is stolen and when it is used. According to the U.S. Government Accountability Office, 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.
>
> *See* GAO Report, at p. 29.

79. Personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

80. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future. This is why Defendants' one-year credit monitoring offering is inadequate.

81. Data breaches are preventable. As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."

82. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

83. Indeed, here Defendants took actions to secure the affected systems *after* the Data Breach, but should have implemented those actions previously to prevent the Data Breach.

84. The types of information Defendants acknowledge were stolen by the criminals are sufficiently sensitive and valuable to identity thieves and criminals in perpetrating identity crimes. This information can be used to perpetrate scams, victimize the persons who own the information, and commit identity theft and fraud.

85. Criminals can use PII to devise and employ phishing and social engineering schemes capitalizing on the genuine information stolen from Defendants to send fraudulent mail and other communications to Plaintiffs and Class members that look authentic, but which are designed to lure them into paying money or providing other information that the criminals can use to steal money.

86. For instance, with a stolen Social Security number, which is only one category of the PII compromised in the Data Breach, someone can open financial accounts, file fraudulent tax returns, commit crimes, and steal benefits.[22]

87. Victims of the Data Breach, like Plaintiffs and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[23]

[22] *See, e.g.*, Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number, Nov. 2, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ (last visited Feb. 4, 2023).
[23] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last visited Feb. 4, 2023).

88. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other information for unauthorized activity for years to come.

89. Plaintiffs and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential information used against them by spam callers to defraud them;

e. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

90. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which remains in the possession of Defendants, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiffs' and Class members' PII.

91. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendants has caused them but, given the kind of PII Defendants made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PII, Plaintiffs and Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[24]

[24] Will a New Social Security Number Affect Your Credit?, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html#:~:text=Will%20a%20new%20Social%20Security,when%20determining%20someone's%20credit%20score. (last visited Feb. 4, 2023).

Defendants Could Have Prevented the Breach but Failed to Adequately Protect the PII of the Plaintiffs and Class Members

92. Data disclosures and data breaches are preventable.[25] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[26] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[27]

93. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[28]

94. Defendants obtained and stored Plaintiffs' and Class members' PII—including but not limited to, their names Social Security numbers—and were entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII.

95. Defendants breached fiduciary duties owed to Plaintiffs and the Class as guardian of their PII.

96. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendants' failure to incur the costs necessary to implement adequate and reasonable cyber

[25] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[26] *Id.*
[27] *Id.*
[28] *Id.*

security training, procedures and protocols that were necessary to protect Plaintiffs' and Class members' PII.

97. Defendants maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

98. Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiffs' and Class members' PII was stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach.

99. The risk of improper disclosure of Plaintiffs' and Class members' PII was a known risk to Defendants, and thus Defendants was on notice that failing to take necessary steps to secure Plaintiffs' and Class members' PII from that risk left the PII in a dangerous condition.

100. Defendants disregarded the rights of Plaintiff and Class members by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

Facts Related to Plaintiff Tanner

101. On or about April 18, 2022 and again on May 4, 2022, Plaintiff Tanner visited Defendants' website to fill out applications for a lease purchase agreement for an item for personal use. Plaintiff Tanner provided his PII to Defendants, including his name, address, Social Security

number, and driver's license number. Defendants never loaned Plaintiff any funds, but retained his PII without any further business purpose.

102. Plaintiff Tanner received a letter from Snap in December 2022, advising him that his PII, including his name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

103. Plaintiff Tanner received notifications in July 2022 and August 2022 that a third party had attempted to open financial accounts in his name with Wells Fargo Bank. Plaintiff had to spend at least 50 hours taking measures to dispute the accounts, prevent the opening of fraudulent accounts using his PII, and reviewing his financial accounts and his credit reports.

104. As a result of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Tanner's PII has been obtained by cybercriminals.

105. Plaintiff Tanner is now under a present an imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Tanner's life. The imminent risk of identity theft and fraud Plaintiff Tanner now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

106. As a result of the Data Breach, Plaintiff Tanner has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Tanner, including (but not limited to) investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, reviewing accounts statements, and monitoring other personal information.

107. As a direct and proximate result of the Data Breach, Plaintiff Tanner will need to have identity theft protection for the foreseeable future.

108. Plaintiff Tanner has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Tanner's PII. Additionally, Plaintiff Tanner's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Sanchez

109. On or about May 2, 2022, Plaintiff Sanchez visited Defendants' website to apply for a lease purchase agreement for an item for personal use. As part of the application process, Plaintiff Sanchez provided his PII to Defendants, including his name, address, Social Security number, and driver's license number. Defendants never loaned Plaintiff any funds but retained his PII without any further business purpose.

110. Plaintiff Sanchez received a letter from Snap in December 2022, advising him that his PII, including his name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

111. As a result of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Sanchez's PII has been obtained by cybercriminals.

112. Plaintiff Sanchez is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Sanchez's life. The imminent

risk of identity theft and fraud Plaintiff Sanchez now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

113. In fact, Plaintiff Sanchez has already experienced identity theft. In or around July 2022, Plaintiff Sanchez discovered that someone was fraudulently using his information, including Social Security number and driver's license number, to work as an Uber driver under Plaintiff's name. Since the Data Breach, Plaintiff Sanchez has also had fraudulent loans applied for in his name.

114. Plaintiff Sanchez had to spend numerous hours taking measures to address the fraudulent activity, including filing a police report, participating in meetings with Uber in an attempt to get the matter resolved, placing credit freezes to prevent the opening of fraudulent loans or accounts, and reviewing his financial accounts and his credit reports.

115. As a result of the Data Breach, Plaintiff Sanchez has also expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Sanchez, including (but not limited to) investigating the Data Breach, investigating how best to protect his information from further identity theft, and monitoring other personal information.

116. As a direct and proximate result of the Data Breach, Plaintiff Sanchez will need to have identity theft protection for the foreseeable future.

117. Plaintiff Sanchez has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Sanchez's PII. Additionally, Plaintiff Sanchez's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful

disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Montgomery

118. In or about 2021, Plaintiff Tameka Montgomery visited Defendants' website to apply for a leasing agreement for an item of furniture for personal use. As part of the application process, Plaintiff Tameka Montgomery provided her PII to Defendants, including her name, address, Social Security number, and driver's license number. Defendants never loaned Plaintiff any funds but retained her PII without any further business purpose.

119. Plaintiff Montgomery received a letter from Snap in December 2022, advising her that her PII, including her name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

120. Plaintiff Montgomery has received multiple alerts that her information was exposed on the dark web including on or about on September 9, 2022. Plaintiff Montgomery had to spend at least 30 hours taking measures as a result of these alerts, including expending time to acquire and use, at $19.00 per month, Experian credit monitoring and the time she has had to devote to reviewing Experian's reports on her credit, and also the time to acquire and use credit protection through Intuit Turbo Tax for $59.00.

121. Because of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Montgomery's PII has been obtained by cybercriminals.

122. Plaintiff Montgomery is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Montgomery's life.

The imminent risk of identity theft and fraud Plaintiff Montgomery now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

123. As a result of the Data Breach, Plaintiff Montgomery has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Montgomery, including (but not limited to) investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, reviewing accounts statements, and monitoring other personal information.

124. As a direct and proximate result of the Data Breach, Plaintiff Montgomery will need to have identity theft protection for the foreseeable future.

125. Plaintiff Montgomery has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Montgomery's PII. Additionally, Plaintiff Montgomery's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Simeon

126. On or about January 4, 2021, Plaintiff Sterling Simeon visited Defendants' website to apply for a lease purchase agreement for an item for personal use. As part of the application process, Plaintiff Simeon provided his PII to Defendants, including his name, address, Social Security number, and driver's license number.

127. Plaintiff Simeon received a letter from Snap in December 2022, advising him that his PII, including his name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

128. Plaintiff Simeon received notifications in June 2022 and December 2022 that a third party had attempted to open financial accounts in his name with American Express and Continental Finance. Plaintiff Simeon had to spend at least 40 hours taking measures to dispute the accounts, prevent the opening of fraudulent accounts using his PII, and reviewing his financial accounts and his credit reports.

129. Because of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Simeon's PII has been obtained by cybercriminals.

130. Plaintiff Simeon is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Simeon's life. The imminent risk of identity theft and fraud Plaintiff Simeon now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

131. As a result of the Data Breach, Plaintiff Simeon has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Simeon, including (but not limited to) investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, reviewing accounts statements, and monitoring other personal information.

132. As a direct and proximate result of the Data Breach, Plaintiff Simeon will need to have identity theft protection for the foreseeable future.

133. Plaintiff Simeon has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Simeon's PII. Additionally, Plaintiff Simeon's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Grayes

134. Plaintiff Grayes applied for credit with Snap. As part of the application process, Plaintiff Grayes provided her PII to Defendants, including her name, address, Social Security number, and driver's license number.

135. Plaintiff Grayes received a letter from Snap in December 2022, advising her that her PII, including her name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

136. Since the breach, Plaintiff Grayes has had to spend numerous hours taking measures to check and confirm her bank and other accounts were secure, contacting credit agencies to ensure her credit was not impacted, and reviewing her financial accounts and her credit reports, among other tasks.

137. Because of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Grayes' PII has been obtained by cybercriminals.

138. Plaintiff Grayes is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Grayes' life. The imminent

risk of identity theft and fraud Plaintiff Grayes now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

139. As a result of the Data Breach, Plaintiff Grayes has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Grayes, including (but not limited to) investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, reviewing accounts statements, and monitoring other personal information.

140. As a direct and proximate result of the Data Breach, Plaintiff Grayes will need to have identity theft protection for the foreseeable future.

141. Plaintiff Grayes has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Grayes' PII. Additionally, Plaintiff Grayes PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Saunders

140. Plaintiff Saunders applied for credit with Snap. As part of the application process, Plaintiff Saunders provided her PII to Defendants, including her name, address, Social Security number, and driver's license number.

141. Plaintiff Saunders received a letter from Snap in December 2022, advising her that her PII, including her name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

142. Since the breach, Plaintiff Saunders has had to spend numerous hours taking measures to check and confirm her bank and other accounts were secure, contacting credit agencies to ensure her credit was not impacted, and reviewing her financial accounts and her credit reports, among other tasks.

143. Because of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Saunders' PII has been obtained by cybercriminals.

144. Plaintiff Saunders' is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Saunders' life. The imminent risk of identity theft and fraud Plaintiff Saunders now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

145. As a result of the Data Breach, Plaintiff Saunders has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Saunders, including (but not limited to) investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, reviewing accounts statements, and monitoring other personal information.

146. As a direct and proximate result of the Data Breach, Plaintiff Saunders will need to have identity theft protection for the foreseeable future.

147. Plaintiff Saunders has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Saunders' PII. Additionally, Plaintiff Saunders' PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Peppelaar

148. Plaintiff Peppelaar financed his purchase of automobile tires through Snap in 2018. As part of Snap's financing application, Plaintiff Peppelaar provided his PII to Defendants, including his name, address, Social Security number, and driver's license number.

149. Plaintiff Peppelaar received a letter from Snap in December 2022, advising him that his PII, including his name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

150. Since the breach, Plaintiff Peppelaar has had to spend numerous hours taking measures to check and confirm his financial accounts were secure, contacting credit agencies regarding his credit score, and reviewing his financial accounts and credit reports, among other tasks.

151. Because of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Peppelaar's PII has been obtained by cybercriminals.

152. Plaintiff Peppelaar is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Peppelaar's life. The

imminent risk of identity theft and fraud Plaintiff Peppelaar now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

153. As a result of the Data Breach, Plaintiff Peppelaar has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Peppelaar, including (but not limited to) investigating the Data Breach, changing cards, switching banks, reviewing accounts statements, and monitoring other personal information.

154. As a direct and proximate result of the Data Breach, Plaintiff Peppelaar will need to have identity theft protection for the foreseeable future.

155. Plaintiff Peppelaar has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Peppelaar's PII. Additionally, Plaintiff Peppelaar's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Schulmeister

156. Plaintiff Schulmeister financed a purchase for earrings through Snap in or about 2020. As part of the financing application process, Plaintiff Schulmeister provided her PII to Defendants, including her name, address, Social Security number, and driver's license number.

157. Plaintiff Schulmeister received a letter from Snap in December 2022, advising her that her PII, including her name and Social Security number, was potentially accessed or acquired by cybercriminals in the Data Breach.

158. Since the breach, Plaintiff has had to spend numerous hours taking measures to check and confirm her bank and other accounts were secure and reviewing her financial accounts and her credit reports, among other tasks.

159. Because of Defendants' negligence and failure to properly secure the PII in their possession, which negligence and failure led to the Data Breach, Plaintiff Schulmeister's PII has been obtained by cybercriminals.

160. Plaintiff Schulmeister is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Schulmeister's life. The imminent risk of identity theft and fraud Plaintiff Schulmeister now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

161. As a result of the Data Breach, Plaintiff Schulmeister has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Schulmeister, including (but not limited to) investigating the Data Breach, reviewing accounts statements, changing her own passwords, signing up for credit monitoring and identity theft insurance, and monitoring other personal information.

162. As a direct and proximate result of the Data Breach, Plaintiff Schulmeister will need to have identity theft protection for the foreseeable future.

163. Plaintiff Schulmeister has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Schulmeister's PII. Additionally, Plaintiff Schulmeister's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Plaintiffs' and Class Members' Damages

164. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

165. Plaintiffs and Class members have or will suffer actual injury as a direct result of the Data Breach including:

a) Spending time reviewing charges for any fraudulent charges and remedying any fraudulent charges found;

b) Purchasing credit monitoring and identity theft prevention;

c) Requesting and reviewing their credit reports;

d) Spending time and money addressing and remedying identity theft;

e) Spending time placing "freezes" and "alerts" with credit reporting agencies and, subsequently, temporarily lifting a security freeze on a credit report, or removing a security freeze from a credit report;

f) Spending time on the phone with or visiting financial institutions to dispute fraudulent charges;

g) Contacting their financial institutions and closing or modifying financial accounts compromised as a result of the Data Breach; and

h) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

166. Moreover, Plaintiffs and Class members have an interest in ensuring that their personal information is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data containing their personal information is secure.

167. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy.

168. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members are at an increased and immediate risk of future harm, including from identity theft and fraud.

169. As a result of the Data Breach, Plaintiffs and Class members are at an imminent risk of identity theft and fraud. This risk will continue to exist for years to come, as Plaintiffs and Class members must spend their time being extra vigilant, due to Defendants' failures, to try to prevent being victimized for the rest of their lives.

170. Because Defendants presented such an easy target to cyber criminals, Plaintiffs and Class members have already been subjected to violations of their privacy and have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now and in the future, spend time to more closely monitor their affected PII to guard against identity theft and other fraud.

171. Plaintiffs and Class members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services or other protective measures to deter and detect identity theft.

CLASS ACTION ALLEGATIONS

172. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5) on behalf of a class of similarly situated individuals (the "Class") defined as follows:

> All persons residing in the United States whose personally identifiable information was accessed or acquired as a result of the Snap data breach that is the subject of the notice of Data Breach that Defendants sent to Plaintiffs and other Class Members (the "Nationwide Class" or "Class").

173. Additionally, Plaintiff Montgomery brings this action pursuant Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5) on behalf of a subclass of similarly situated individuals defined as follows:

> All Illinois residents whose PII was accessed on Defendants' system(s) in the Data Breach and who were sent a notice of the Data Breach (the "Illinois Subclass").

174. Additionally, Plaintiffs Simeon, Grayes, and Saunders bring this action pursuant Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5) on behalf of a subclass of similarly situated individuals defined as follows:

> All California residents whose PII was accessed on Defendants' system(s) in the Data Breach and who were sent a notice of the Data Breach (the "California Subclass").

175. Excluded from the Class and Subclasses are Defendants; any entity in which either Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by either Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families.

176. Plaintiffs reserve the right to modify and/or amend the Class definition, including but not limited to creating subclasses, as necessary.

177. ***Numerosity***. The Class members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class members are unknown at this time, public news reports indicate that approximately 61,302 individuals had their PII compromised in this Data Breach. The identities of Class members are ascertainable through Defendants' records, Class members' records, publication notice, self-identification, and other means.

178. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class members;

b. Whether Defendants had a duty not to disclose the PII of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendants had a duty not to use the PII of Plaintiffs and Class members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class members are entitled to actual damages, nominal damages, treble damages, and/or exemplary damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

179. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class members because Plaintiffs, like all Class members, had his PII compromised, breached and stolen in the Data Breach. Plaintiffs and Class members were injured through Defendants' uniform misconduct described in this Complaint and assert the same claims for relief.

180. ***Adequacy***. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel who are experienced in class actions and complex litigation, including data privacy litigation of this kind. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

181. ***Predominance***. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

182. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class members have been harmed by Defendants' wrongful conduct and/or action.

183. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. No difficulties would be encountered in this litigation that would preclude its maintenance as a class action.

184. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

185. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2), because Defendants have acted or refused to act on grounds that apply generally to the Class so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiffs and the Nationwide Class)

186. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 185 with the same force and effect as though fully set forth herein.

187. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

188. Defendants had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class members' PII.

189. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class members could and would suffer if the data were wrongfully disclosed.

190. Defendants' actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiffs and Class members. Defendants knew, or should have known, of the risks inherent in collecting and storing the personal information of Plaintiffs and Class members and the importance of adequate security in storing the information. Additionally, Defendants are aware of numerous, well-publicized data breaches that exposed the personal information of individuals.

191. Defendants had a common law duty to prevent foreseeable harm to Plaintiffs' and Class members' PII. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Defendants to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' personal information would not be unsecured and accessible by unauthorized persons.

192. Defendants had a special relationship with Plaintiffs and Class members. Defendants were entrusted with Plaintiffs' and Class members' personal information, and Defendants were in a position to protect the personal information from unauthorized access.

193. The duties of Defendants also arose under section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Defendants.

194. Defendants had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal information in their possession so that the PII would not come within the possession, access, or control of unauthorized persons.

195. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and Class members, the critical importance of providing adequate security of that data, and the necessity for encrypting all data stored on Defendants' systems.

196. More specifically, the duties of Defendants included, among other things, the following duties, and Defendants carelessly and negligently acted or failed to act in one or more of the following ways:

a. Failing to conduct proper and reasonable due diligence over their data security systems, practices, and procedures;

b. Failing to adopt, implement, and maintain adequate security measures for protecting an individual's personal information to ensure that the information is not accessible online by unauthorized persons;

c. Failing to adopt, implement, and maintain adequate security measures for deleting or destroying personal information when Defendants' business needs no longer required such information to be stored and maintained; and

d. Failing to adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches, and notify affected persons without unreasonable delay.

197. Defendants breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting personal information in their possession so that the information would not come within the possession, access, or control of unauthorized persons.

198. Defendants acted with reckless disregard for the security of the personal information of Plaintiffs and Class members because Defendants knew or should have known that their data security was not adequate to safeguard the personal information that was collected and stored.

199. Defendants acted with reckless disregard for the rights of Plaintiffs and Class members by failing to promptly detect the Data Breach, and further, by failing to notify Plaintiffs and Class members of the Data Breach in the most expedient time possible and without unreasonable delay pursuant to common law duties to provide reasonably timely and truthful data-breach notification, so that Plaintiffs and Class members could promptly take measures to protect themselves from the consequences of the unauthorized access to the personal information compromised in the Data Breach.

200. As a result of the unlawful conduct of Defendants, Plaintiffs and Class members have suffered and will continue to suffer foreseeable harm, including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Negligence Per Se
(On behalf of Plaintiffs and the Nationwide Class)

201. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 200 with the same force and effect as though fully set forth herein.

202. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data breach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For

example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One Data Security Breach Litigation*, 488 F. Supp. 3d at 407.

203. Defendants also engaged in conduct declared unlawful under the Safeguards Rule, 16 C.F.R. part 314, promulgated by the FTC pursuant to authority delegated by Congress under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b), to establish standards for financial institutions relating to administrative, technical, and physical safeguards for nonpublic information, including Plaintiff's and Class members' PII.

204. 16 C.F.R. § 314.4 provides:

> In order to develop, implement, and maintain your information security program, [a financial institution] shall:
>
> (a) Designate an employee or employees to coordinate your information security program.
>
> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> (1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

205. The Safeguards Rule is a process-based rule drafted using intentionally broad language and not incorporating any specific information security standard or framework to allow financial institutions flexibility to "shape the information security programs to their particular

business and to allow the programs to adapt to changes in technology and threats to the security and integrity of customer information."[29]

206. Defendants are financial institutions.

207. Plaintiffs' and Class members' nonpublic personal information was and is customer information.

208. Defendants committed unlawful acts by failing to comply with the requirements of the Safeguards Rule, including but not limited to, failing to:

- Upgrade and maintain their data security systems in a meaningful way so as to prevent the Data Breach;
- Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;
- Block all inbound and outbound Internet, email, and network traffic to foreign countries;
- Maintain a secure firewall configuration;
- Monitor for suspicious or irregular traffic to servers;
- Monitor for suspicious credentials used to access servers;
- Monitor for suspicious or irregular activity by known users;
- Monitor for suspicious or unknown users;
- Monitor for suspicious or irregular server requests;
- Monitor for server requests for personal and financial information;

[29] Fed. Trade Comm'n, Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158, 13159 (Apr. 4, 2019), also available at https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer- information. (last visited Feb. 8, 2023).

- Monitor for server requests from VPNs;
- Monitor for server requests from Tor exit nodes;
- Identify all connections to the computers where Defendants store sensitive information;
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- Scan computers on Defendants' network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;
- Pay particular attention to the security of Defendants' web applications—the software used to give information to visitors to their websites and to retrieve information from them;
- Use a firewall to protect Defendants' computers from hacker attacks while they are connected to a network, especially the Internet;
- Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;
- Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides

is only as effective as its access controls, they should be reviewed periodically;

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

209. Plaintiffs' and Class members' PII was and is nonpublic personal information and customer information.

210. Plaintiffs and Class members are in the group of persons the FTC Act and Safeguards Rule were enacted and implemented to protect, and the harms they suffered in the Data Breach were the types of harm they were designed to prevent.

211. As a result of the conduct of Defendants that violated the FTC Act and Safeguards Rule, Plaintiffs and Class members have suffered and will continue to suffer foreseeable harm. Plaintiffs and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other

forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class)

212. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 211 with the same force and effect as though fully set forth herein.

213. In connection with the dealings Plaintiffs and Class members had with Snap, Plaintiffs and Class members entered into implied contracts with Snap.

214. Pursuant to these implied contracts, Plaintiffs and Class members provided Snap with their PII in order for Snap to provide financing services. In exchange, Snap agreed to, among other things, and Plaintiffs and Class members understood that Snap would: (1) provide services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members PII in compliance with federal and state laws and regulations and industry standards.

215. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Snap, on the other hand. Indeed, Snap was clear in its Privacy Policy, and Plaintiff understood that Snap supposedly respects and is committed to protecting customer privacy.

216. Had the Plaintiffs and Class members known that Snap would not adequately protect its clients' customers' and former customers' PII, they would not have provided Snap or Snap's clients with their PII.

217. Plaintiffs and Class members performed their obligations under the implied contracts when they provided Snap with their PII, either directly or indirectly.

218. Snap breached its obligations under their implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

219. Snap's breach of its obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

220. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and Class members 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 and non-economic harm.

221. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class members sustained damages as alleged herein.

222. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

COUNT IV
Invasion of Privacy
(On behalf of the Plaintiffs and the Nationwide Class)

223. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 222 with the same force and effect as though fully set forth herein.

224. The State of Utah recognizes the tort of invasion of privacy:

> The elements of an invasion-of-privacy claim are: (1) the disclosure of the private facts must be a public disclosure and not a private one; (2) the facts disclosed to the public must be private facts, and not public ones; (3) the matter made public must be one that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.

See Shattuck-Owen v. Snowbird Corp, 2000 UT 94, 16 P.3d 555 (2000) (citing *Stien v. Marriott Ownership Resorts, Inc*., 944 P.2d 374, 380 (Utah Ct. App. 1997) (quoting W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 117 856–57 (5th ed.1984) (footnote omitted))).

225. Plaintiffs and Class members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

226. Defendants owed a duty to Plaintiffs and Class members to keep their PII confidential.

227. Defendants intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII of Plaintiffs and Class members.

228. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class members, by way of Defendants' failure to protect the PII.

229. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class members is highly offensive to a reasonable person.

230. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class members disclosed their PII to Defendants as part of their relationships with Defendants, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

231. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiffs' and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

232. Defendants acted with intention and a knowing state of mind when they permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

233. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class members.

234. As a proximate result of the above acts and omissions of Defendants, PII of Plaintiffs and Class members was disclosed to third parties without authorization, causing Plaintiffs and Class members to suffer damages.

235. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class members have no adequate remedy

at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class members.

COUNT V
Unjust Enrichment
(On behalf of the Plaintiffs and the Nationwide Class)

236. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 235 with the same force and effect as though fully set forth herein.

237. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

238. Plaintiffs and Class members conferred a monetary benefit to Defendant when they provided their PII to receive Defendants' services.

239. Defendants knew that Plaintiffs and Class members conferred a monetary benefit to Defendants when they accepted and retained that benefit. Defendants profited from this monetary benefit, as the transmission of PII to those companies to whom Defendants makes service referrals is an integral part of Defendants' business. Without transmitting Plaintiffs' and Class members' PII to third-parties, Defendants would have dramatically diminished business and profits.

240. Defendants were supposed to use some of the monetary benefit provided to them from Plaintiffs and Class members to secure the PII belonging to Plaintiffs and Class members by paying for costs of adequate data management and security.

241. Defendants should not be permitted to retain any monetary benefit belonging to Plaintiffs and Class members because Defendants failed to implement necessary security measures to protect the PII of Plaintiff and Class members.

242. Defendants gained access to the Plaintiffs' and Class members' PII through inequitable means because Defendants failed to disclose that it used inadequate security measures.

243. Plaintiffs and Class members were unaware of the inadequate security measures and would not have provided their PII to Defendants had they known of the inadequate security measures.

244. To the extent that this cause of action is pled in the alternative to the others, Plaintiffs and Class members have no adequate remedy at law.

245. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which 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 of Plaintiffs and Class members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

246. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

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

COUNT VI
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class)

248. Plaintiffs repeat and reallege the allegations contained in Paragraphs 1 through 247 with the same force and effect as though fully set forth herein.

249. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

250. Defendants owed and owe a duty of care to the Plaintiffs and Class members that require they to adequately secure Plaintiff's and Class members' PII.

251. Defendants still possess the PII of the Plaintiffs and the Class members.

252. Defendants have not satisfied their contractual obligations and legal duties to the Plaintiffs and the Class members.

253. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to the Plaintiffs and the members of the Class. Further, the Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

254. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

255. The Plaintiffs and the Class, therefore, seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third party security auditors;

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

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants provide employee training regarding the dangers and risks inherent in using file-sharing websites;

e. Ordering that Defendants cease transmitting PII via file-sharing websites;

f. Ordering that Defendants cease storing PII on file-sharing websites;

g. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for their provision of services;

h. Ordering that Defendants conduct regular database scanning and security checks; and

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, personally identifiable information.

COUNT VII
VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT,
815 Ill. Comp. Stat. § 505/1, *et seq*. ("CFA")
(On Behalf of Plaintiff Tameka Montgomery and the Illinois Subclass Against All Defendants)

256. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 255 with the same force and effect as though fully set forth herein.

257. Plaintiff Montgomery brings this claim on behalf of herself and the Illinois Subclass. This Count is brought against Defendants.

258. Plaintiff Montgomery and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Illinois Subclass, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

259. Defendants are engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

260. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff and the Illinois Subclass's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting material facts to Plaintiff and the Illinois Subclass regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff Montgomery and the Illinois Subclass; (3) failing to disclose or omitting material facts to Plaintiff and the Illinois Subclass about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and

security of the PII of Plaintiff Montgomery and the Illinois Subclass; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Montgomery's and the Illinois Subclass's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

261. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Montgomery and the Illinois Subclass and defeat their reasonable expectations about the security of their PII.

262. Moreover, Defendants represented that they would maintain the data they collected in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

263. Defendants intended that Plaintiff Montgomery and the Illinois Subclass rely on their deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of goods and services.

264. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Illinois Subclass. Plaintiff Montgomery and the Illinois Subclass have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

265. Defendants also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff Montgomery and the Illinois Subclass of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*

266. As a result of Defendants' wrongful conduct, Plaintiff Montgomery and the Illinois Subclass were injured in that they never would have provided their PII to Defendants, or purchased

267. Defendants' services, had they known or been told that Defendants failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

268. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff Montgomery and the Illinois Subclass have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendants that Plaintiff Montgomery and the Illinois Subclass would not have made had they known of Defendants' inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

269. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Montgomery and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the CFA.

COUNT VIII
VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT, Cal. Civ. Code § 1798.100, *et seq*. ("CCPA")
(On Behalf of Plaintiff Simeon and the California Subclass Against All Defendants)

270. Plaintiff Simeon repeats and realleges the allegations of Paragraphs 1 through 269 with the same force and effect as though fully set forth herein.

271. This Count is brought on behalf of Plaintiff Simeon and the California Subclass against all Defendants.

272. Defendants violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent the PII of Plaintiff Simeon and the California Subclass from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of

their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

273. The non-redacted and non-encrypted PII of Plaintiff Simeon and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendants' violations of their duty under the CCPA.

274. Plaintiff Simeon and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendants' acts described above.

275. Defendants knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff Simeon and members of the California Subclass was exposed.

276. Defendants are organized for the profit or financial benefit of their owners and collect PII as defined in Cal. Civ. Code § 1798.140.

277. Plaintiff Simeon and the California Subclass seek injunctive or other equitable relief to ensure that Defendants hereinafter adequately safeguard PII by implementing reasonable security procedures and practices. This relief is important because Defendants still hold PII related to Plaintiff Simeon and the California Subclass. Plaintiff Simeon and the California Subclass have an interest in ensuring that their PII is reasonably protected.

278. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Simeon gave written notice to Defendants of their specific violations of section 1798.150(a) by certified mail dated December 14, 2022. Pursuant to § 1798.150(b) of the CCPA. Under § 1798.150(b):

> Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.

279. Defendants did not respond at all to Plaintiff Simeon's December 14, 2022 CCPA notice. Defendants therefore did not give Plaintiff Simeon an "express written statement," and did not "actually cure" the effects of the Data Breach within 30 days of delivery of the CCPA notice letter (which Plaintiff Simeon believes any such cure is not possible under these facts and circumstances).

280. Because Defendants have not "actually cured" the violation, nor have they suppled an "express written statement," Plaintiff Simeon seeks statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT IX
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.*

(On Behalf of Plaintiffs Simeon, Grayes and Saunders and the California Subclass Against All Defendants)

281. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 280 with the same force and effect as though fully set forth herein.

282. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

283. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

284. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

285. Plaintiffs Simeon, Grayes and Saunders and members of the California subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendants, directly and/or indirectly, for the purpose of obtaining a service from Defendants.

286. The personal information of Plaintiffs and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendants collect and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of

a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

287. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs Simeon, Grayes and Saunders and the California subclass. Specifically, Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiffs Simeon, Grayes and Saunders and the California subclass from unauthorized access, destruction, use, modification, or disclosure. Defendants further subjected Plaintiffs Simeon's, Grayes' and Saunders' and the California subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendants' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

288. As a direct and proximate result of Defendants' violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiffs Simeon, Grayes and Saunders and the California subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiffs Simeon, Grayes and Saunders and the California subclass by the

ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

289. As a direct and proximate result of Defendants' acts or omissions, Plaintiffs Simeon, Grayes and Saunders and the California subclass were injured and lost money or property including, but not limited to, the loss of Plaintiffs' and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiffs seek compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

290. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

291. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

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

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

c. If the information is possible to determine at the time the notice is provided, then any of the following:

   i. the date of the breach,

   ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

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

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

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

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

292. Defendants failed to provide the legally compliant notice under § 1798.82(d) to Plaintiffs Simeon, Grayes and Saunders and members of the California subclass. On information and belief, to date, Defendants have not sent written notice of the data breach to all impacted individuals. As a result, Defendants have violated § 1798.82 by not providing legally compliant and timely notice to Plaintiffs and Class members. The breach was continuous and ongoing for several months over the summer of 2022 and Defendants determined Plaintiffs' and Class member's data was part of the breach in October 2022, but failed to timely disclose the breach of Plaintiffs and class members until December 2022. Plaintiffs and Class members could have taken

action to protect their personal information during this long period, but were unable to do so because they were not timely notified of the breach.

293. On information and belief, many Class members affected by the breach, have not received any notice at all from Defendants in violation of Section 1798.82(d).

294. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiffs Simeon, Grayes and Saunders and Class members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

295. As a direct consequence of the actions as identified above, Plaintiffs Simeon, Grayes and Saunders and the California subclass members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT X
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §17200, *et seq.*.

(On Behalf of Plaintiffs Simeon, Grayes and Saunders and the California Subclass Against All Defendants)

296. Plaintiffs repeat and reallege the allegations of Paragraphs 1 through 295 with the same force and effect as though fully set forth herein.

297. Defendants are a "person" defined by Cal. Bus. & Prof. Code § 17201.

298. Defendants violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

299. Defendants' "unfair" acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiffs' and California sublcass members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of Defendants' data breach. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendants' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

300. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law.

301. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California subclass members' personal information, which was a direct and proximate cause of Defendants' data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of Defendants' data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of Defendants' data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California subclass members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California subclass members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

302. 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' personal information.

303. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiffs Simeon, Grayes and Saunders and California subclass members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages 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 personal information.

304. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable.

305. Plaintiffs Simeon, Grayes and Saunders and class members have lost money and property as a result of Defendants' conduct in violation of the UCL, as stated herein and above.

306. By deceptively storing, collecting, and disclosing their personal information, Defendants have taken money or property form Plaintiffs and class members.

307. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

308. Plaintiffs Simeon, Grayes and Saunders and California subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs Tracy Tanner, Victor Sanchez, Tameka Montgomery, Sterling Simeon, Monique Grayes and Carolyn Saunders individually and on behalf of the Class, requests that the Court:

A. Certify this case as a class action on behalf of the Class defined above, appoint the Plaintiffs as the Class representative and Subclass Representatives, as applicable, and appoint the undersigned counsel as Class counsel;

B. Award equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of the Plaintiffs and Class Members;

C. Award injunctive relief as requests by the Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

vi. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

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

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

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

xi. requiring Defendants to conduct regular database scanning and securing checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment

D. Award the appropriate monetary relief to the Plaintiffs and Class members, including actual damages, nominal damages, statutory damages, consequential damages, treble damages, punitive damages, restitution, and all other such and further monetary relief as is just and proper;

E. Award Plaintiff and Class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

F. Award Plaintiff and Class members pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs Tracy Tanner, Victor Sanchez, Tameka Montgomery, Sterling Simeon, Monique Grayes Carolyn Saunders, Nick Peppelaar, and Tara Schulmeister demand a trial by jury of any and all issues in this action so triable of right.

Dated: February 9, 2023

Respectfully Submitted,

/s/William B. Federman

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560/(405) 239-2112 (facsimile)
wbf@federmanlaw.com

M. Anderson Berry*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com

Brian D. Flick*
DANNLAW
15000 Madison Avenue
Lakewood, OH 44107
Telephone: (513) 645-3488
Facsimile: (216) 373-0536
bflick@dannlaw.com

*Admitted Pro Hac Vice

Interim Class Counsel for the Plaintiffs and Putative Class

Charles H. Thronson, USB 3260
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, UT 84111
Telephone: (801) 532-1234
Facsimile: (801) 536-6111
CThronson@parsonsbehle.com

Liaison Counsel for the Plaintiffs and Putative Class

JASON M. WUCETICH**
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201
jason@wukolaw.com

Gary M. Klinger**
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

** Pro Hac Vice application forthcoming

Additional Counsel for Plaintiffs and Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on February 9, 2023, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using CM/ECF. Copies of the foregoing document will be served upon interested counsel via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ William B. Federman
William B. Federman