Steven A. Christensen, #5190
Cameron S. Christensen #16015
Christensen Young & Associates, PLLC
9980 South 300 West #200
Sandy, UT 84070
Telephone: (801) 255-8727
Facsimile: (888) 569-2786
steven@christensenyounglaw.com
cameron@christensenyounglaw.com
[additional counsel listed on signature block]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

TRACY TANNER, individually and on behalf of all others similarly situated, Plaintiff, v. **SNAP FINANCE LLC,** and **SNAP RTO LLC** Defendants.	Civil Action No. **CLASS ACTION COMPLAINT FOR DAMAGES** (with Jury Demand Requested)

Plaintiff Tracy Tanner ("Plaintiff" or "Tanner"), individually and on behalf of all others similarly situated, through counsel, brings this action against Defendants Snap Finance LLC ('SF") and Snap RTO LLC ("SP") (collectively, "Defendants"), and alleges upon personal knowledge as to his 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 Plaintiff's 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 Plaintiff and Class members.

2. Defendants are finance companies that offer direct loans and secured financing to consumers across the United States.

3. On December 1, 2022, Defendants sent to Plaintiff and Class members a letter entitled "Notice of Security Incident" ("Notice"). *See* Notice, attached hereto as Exhibit 1. 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––Plaintiff and Class members—until December 1, 2022.

4. The Data Breach exposed Plaintiff's 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, Plaintiff and Class members reasonably 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 Plaintiff and Class members is referred to herein as "PII."

5. 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 Plaintiff 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.

6. Plaintiff 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."[1]

7. 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 acquired electronic files containing the PII of Plaintiff 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 Plaintiff and Class members of the Data Breach until on or around December 1, 2022.

[1] *See* https://snapfinance.com/legal/privacy.

8. Plaintiff, individually, and on behalf of all persons similarly situated, seeks 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. Plaintiff 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 Plaintiff's and Class members' PII.

PARTIES, JURISDICTION, AND VENUE

9. Plaintiff Tracy Tanner is a resident and citizen of Ohio.

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

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

12. 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 Plaintiff, are citizens of different states from Defendants.

13. 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.

GENERAL ALLEGATIONS

The Data Breach

14. On or about December 1, 2022, Defendants provided the Notice to Plaintiff and Class members. In the Notice, Defendants state that between June 23, 2022 and September 8,

2022, an unauthorized third party acquired information from some of Defendants' systems that contain the PII of Plaintiff and Class members.

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

16. The Notice states that Plaintiff's 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.

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

18. 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 in the Data, at the time they completed their "review" of the scope and extent of the Data Breach.

Industry Standards for Data Security

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

20. 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 Plaintiff's and Class members' PII.

21. Because of Defendants' failure to implement, maintain, and comply with necessary cybersecurity requirements, Defendants were unable to protect Plaintiff's 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 Plaintiff's and Class members' PII in the Data Breach without being stopped.

22. 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 Plaintiff and Class members. Discovery on Defendants, law enforcement investigators, and private investigators, will reveal more specific facts about Defendants' deficient and unreasonable security procedures.

23. 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.

24. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[2] and protection of personal information[3] which includes basic security standards applicable to all types of businesses.

25. 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;

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;

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

[3] *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.

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.

26. 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.[4]

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

28. Plaintiff 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.

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

30. 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;

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

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;

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.

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

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

32. 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.

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

34. 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

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

36. 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.

37. 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.

38. 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.[5]

39. 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. Plaintiff's and Class members' personal data that was stolen has a high value on both legitimate and black markets.

40. 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

[5] *See* https://www.gao.gov/assets/gao-07-737.pdf at 29.

the life blood, the free flow of information.[6]

41. 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.

42. 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.[7] The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[8] 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.

43. 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.

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

---

[6] 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.

[7] 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.

[8] *Id.*

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

Damages from Data Breaches

46. 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.

47. 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.

48. 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."

49. 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.

50. 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 Plaintiff 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.

51. 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.

52. 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 blackmarket" for years.

53. 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 Plaintiff 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.

54. 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 . . . ."

55. "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."

56. 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.

57. The types of information Defendants acknowledges 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.

58. 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 Plaintiff 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.

Facts Related to Plaintiff

59. On or about April 18, 2022 and again on May 4, 2022, Plaintiff visited Defendants' website to fill out applications for a lease purchase agreement for an item for personal use. Plaintiff 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.

60. Plaintiff 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.

Plaintiff's and Class Members' Damages

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

62. Plaintiff 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.

63. Moreover, Plaintiff 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.

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

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

66. As a result of the Data Breach, Plaintiff and Class members are at an imminent risk of identity theft and fraud. This risk will continue to exist for years to come, as Plaintiff 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.

67. Because Defendants presented such an easy target to cyber criminals, Plaintiff 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. Plaintiff 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.

68. Plaintiff 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

69. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23 on behalf of a class of similarly situated individuals (the "Class") defined as follows:

> All individuals in the United States whose personally identifiable information was accessed in the Data Breach announced by Defendants.

70. Excluded from the Class 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.

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

72. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. The identities of all Class members are ascertainable through Defendants' records. According to the Texas Attorney General's website, 6,733 Texas residents are Class members. https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

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

- Whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class members;
- Whether Defendants had a duty not to disclose the PII of Plaintiff and Class members to unauthorized third parties;
- Whether Defendants had a duty not to use the PII of Plaintiff and Class members for non-business purposes;
- Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class members;
- When Defendants actually learned of the Data Breach;
- Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised;
- Whether Defendants violated the law by failing to promptly notify Plaintiff and Class members that their PII had been compromised;
- 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;

- Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- Whether Plaintiff and Class members are entitled to actual damages, nominal damages, and/or exemplary damages as a result of Defendants' wrongful conduct;
- Whether Plaintiff and Class members are entitled to restitution as a result of Defendants' wrongful conduct; and
- Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

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

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

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

77. ***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. Plaintiff and Class members have been harmed by Defendants' wrongful conduct and/or action.

78. 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.

79. 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.

80. 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.

COUNT I
Negligence

81. Plaintiff repeats and realleges the allegations of the paragraphs 1–80 with the same force and effect as though fully set forth herein.

82. Defendants' actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiff and Class members. Defendants knew, or should have known, of the risks inherent in collecting and storing the personal information of Plaintiff 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.

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

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

85. 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.

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

87. 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.

88. 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.

89. Defendants acted with reckless disregard for the security of the personal information of Plaintiff 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.

90. Defendants acted with reckless disregard for the rights of Plaintiff and Class members by failing to promptly detect the Data Breach, and further, by failing to notify Plaintiff 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 Plaintiff 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.

91. As a result of the unlawful conduct of Defendants, Plaintiff 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, Plaintiff 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

92. Plaintiff repeats and realleges the allegations of paragraphs 1–80 with the same force and effect as though fully set forth herein.

93. "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 beach 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.

94. 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.

95. 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.

96. 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."[9]

97. Defendants are financial institutions.

98. Plaintiff's and Class members' nonpublic personal information was and is customer information.

99. 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

[9] 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.

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;
- 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.

100. Plaintiff's and Class members' PII was and is nonpublic personal information and

customer information.

101. Plaintiff 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.

102. As a result of the conduct of Defendants that violated the FTC Act and Safeguards Rule, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff 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, Plaintiff 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

103. Plaintiff repeats and realleges the allegations of paragraphs 1–80 with the same force and effect as though fully set forth herein.

104. Defendants acquired and maintained the PII of Plaintiff and Class members.

105. At the time Defendants acquired the PII of Plaintiff and Class members, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the PII using reasonable security measures and not take unjustified risks when collecting, digitizing, and storing the PII.

106. Plaintiff and Class members would not have entrusted their PII to Defendants had they known that Defendants would make the PII vulnerable and fail to take reasonable precautions, such as encrypting the data while in storage, and deleting PII that was no longer necessary.

107. Defendants promised to comply with industry standards and to ensure that Plaintiff's and Class members' PII would remain protected.

108. Implicit in the agreements between Plaintiff and Class members and Defendants to provide their PII to Defendants was Defendants' obligation to:

a. Use the PII for business purposes only;

b. Take reasonable steps to protect and safeguard the PII from known and foreseeable risks;

c. Prevent unauthorized disclosures of the PII;

d. Provide Plaintiff and Class members with prompt and sufficient notice of instances where unauthorized access to the PII is reasonably suspected; and

e. Reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosures or uses.

109. In collecting and maintaining the PII of Plaintiff and Class members and publishing and disseminating privacy policies, Defendants entered into contracts to protect and keep security over the PII of Plaintiff and Class members.

110. Plaintiff and Class members fully performed under their contract with Defendants.

111. Defendants breached the contracts by failing to protect and keep private the personal information of Plaintiff and Class members, including by failing to: (i) encrypt or tokenize the sensitive PII of Plaintiff and Class members, (ii) delete such PII that Defendants no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the Internet where such

accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

112. Defendants also breached a duty to provide reasonably expedient and sufficient notification of the Data Breach.

113. As a result of Defendants' breach of implied contract, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff 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, Plaintiff 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 IV
Invasion of Privacy

114. Plaintiff repeats and realleges the allegations of paragraphs 1–80 with the same force and effect as though fully set forth herein.

115. 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))).

116. Plaintiff and Class members had a reasonable expectation of privacy in the PII that Defendants mishandled.

117. Defendants' conduct as alleged above intruded upon Plaintiff's and Class members' seclusion under common law.

118. By intentionally failing to keep Plaintiff's and Class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class members' private affairs in a manner that identifies Plaintiff and Class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class members.

119. Defendants knew that an ordinary person in Plaintiff's or a Class member's position would consider Defendants' intentional actions to be highly offensive and objectionable.

120. Defendants invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' seclusion by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

121. Defendants intentionally concealed from Plaintiff and Class members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

122. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted.

123. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and Class members' protected privacy interests, caused anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

124. In failing to protect Plaintiff's and Class members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private.

PRAYER FOR RELIEF

WHEREFORE Plaintiff Tracy Tanner, 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 Plaintiff as the Class representative, and appoint the undersigned counsel as Class counsel;

B. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members;

C. Award restitution and damages to Plaintiff and Class members in an amount to be determined at trial;

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff Tracy Tanner demands a trial by jury of any and all issues in this action so triable of right.

Plaintiff Tracy Tanner, individually and on behalf of all others similarly situated,

By: */s/ Steven A. Christensen*
Steven A. Christensen
Cameron S. Christensen
Christensen Young & Associates, PLLC
9980 South 300 West #200
Sandy, UT 84070
Telephone: (801) 255-8727
Facsimile: (888) 569-2786
steven@christensenyounglaw.com
cameron@christensenyounglaw.com

Thomas A. Zimmerman, Jr.*
Jeffrey Blake*
**Pro Hac Vice Applications to be submitted*
Zimmerman Law Offices, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Telephone: (312) 440-0020
www.attorneyzim.com
Email: *firm@attorneyzim.com*

Marc E. Dann*
Brian D. Flick*
**Pro Hac Vice Applications to be submitted*
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Telephone: (216) 373-0539
Email: *notices@dannlaw.com*

Counsel for Plaintiff Tracy Tanner and the putative Class

EXHIBIT 1

snap! finance

December 01, 2022

18351 S00000 135628AB01-A-2 A-02-9GF-DM-18351-58

TRACY TANNER

[redacted]

NOTICE OF SECURITY INCIDENT

Dear Tracy Tanner,

Snap Finance LLC and Snap RTO LLC ("Snap") write to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so. Snap takes the data privacy of our merchants and customers very seriously. We are committed to keeping your personal information secure, and we apologize to you for any concern and frustration this incident may cause.

What Happened? Earlier this year, Snap discovered suspicious activity in its environment. Upon learning this, Snap immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that there was unauthorized access to our environment between June 23, 2022 and September 8, 2022. The investigation also determined that an unauthorized actor had the ability to access certain information stored on the network during this period of time. Therefore, Snap undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related. On October 28, 2022, Snap completed this review and determined the data contained certain information related to you.

What Information Was Involved? Snap determined the type of information potentially impacted by this incident includes your: name, Social Security number, driver's license number or state identification number, and financial account number.

What We Are Doing. Snap takes the confidentiality, privacy, and security of information in its care seriously. Upon discovery of the incident, we immediately commenced an investigation and took steps to implement additional safeguards and reviewed our policies and procedures relating to data privacy and security.

In an abundance of caution, Snap is providing you with access to 12 months of identity monitoring services through Kroll at no cost to you. A description of the services and instructions on how to activate can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the activation process yourself as we are not permitted to activate these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* for general guidance. In addition, you can activate the complimentary identity monitoring services being offered through Kroll. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, or need assistance, please call (855) 504-3723, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding major U.S. holidays). You may also write to Snap at 1193 West 2400 South, West Valley City, Utah, 84119.

Sincerely,

Bryan Allen,
Chief Legal Officer

ELN-162