Exhibit A2

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

IN RE SOVOS COMPLIANCE DATA SECURITY INCIDENT LITIGATION	**Case No. 1:23-cv-12100 ("Master Docket")** **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Sergei Stadnik, Julianne Yenca, James Lawler, and Tony Anderson ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Sovos Compliance, LLC, ("Sovos") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Sovos for its failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' names, dates of birth, Social Security numbers, and account numbers (the "Private Information" or "PII") from hackers.

2. Sovos, which is based in Wilmington, Massachusetts, is a digital regulatory compliance company. As part of its business, and in order to earn profits, Sovos obtained and stored the Private Information of Plaintiffs and Class Members.

3. On or about July 13, 2023, Sovos filed its first of four official notices of data security incident with the Maine Attorney General, followed by subsequent notices on August 23, 2023, September 5, 2023, and September 22, 2023.[1]

4. Beginning on or around August 30, 2023, Sovos also sent out data breach notice letters (the "Notice") to individuals whose Private Information was compromised as a result of the Data Breach.

5. The Notice stated Sovos detected unusual activity on some of its computer systems on or around May 31, 2023, in response to which it "took the affected application offline," launched an investigation, and notified law enforcement. The investigation revealed that unauthorized third parties had access to certain files that contained sensitive clients' customer's information ("the Data Breach"). That access occurred because of vulnerabilities existing in the MOVEit file-transfer software Sovos used in the ordinary course of its business.

6. The unauthorized users had access to Plaintiffs' and approximately 480,000 other individuals highly sensitive Private Information stored on Sovos' systems.

7. As a result of Sovos' inability to timely detect the Data Breach, Plaintiffs and "Class Members" (defined below) had no idea for more than two months that their Private Information had been compromised, and that they were at significant risk of experiencing identity theft and various other forms of personal, social, and financial harm. This substantial and imminent risk will remain for their respective lifetimes.

8. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including, but not limited to, customers' names,

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/c6833f76-d8a7-4a4e-a5b3-130e914e8681.shtml; https://apps.web.maine.gov/online/aeviewer/ME/40/414eb7d6-ef51-4cb8-bcbf-d6bbc69fcf5e.shtml; https://apps.web.maine.gov/online/aeviewer/ME/40/761ef309-bd27-4146-b486-a2a540562e10.shtml; https://apps.web.maine.gov/online/aeviewer/ME/40/9b39fcf4-1dfb-4b64-b5ef-c8144121f70f.shtml.

dates of birth, Social Security numbers, and account numbers that Sovos collected and maintained from its clients.

9. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. There has been no assurance offered by Sovos that all personal data or copies of data have been recovered or destroyed, or that Sovos has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

11. Therefore, Plaintiffs and Class Members have suffered, and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Plaintiffs brings this class action lawsuit to address Sovos' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to timely detect the Data Breach.

13. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Sovos, and thus it was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

14. Upon information and belief, Sovos failed to properly monitor its systems and implement adequate data security practices with regard such systems that housed the Private Information. Had Sovos properly monitored its network systems and implemented such practices, it could have prevented the Data Breach or at least discovered it sooner.

15. Plaintiffs' and Class Members' identities are now at risk because of Sovos' negligent conduct as the Private Information that Sovos collected and maintained is now in the hands of data thieves and other unauthorized third parties.

16. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and compromised during the Data Breach.

17. Accordingly, Plaintiffs, on behalf of themselves and the Classes (defined below), assert claims for negligence, negligence *per se*, breach of third-party beneficiary contract, unjust enrichment, state statutory violations, and declaratory and injunctive relief.

II. PARTIES

18. Plaintiff Sergei Stadnik is, and at all times mentioned herein was, an individual citizen of the State of Arizona. He entrusted his PII to Defendant through his affiliation with one of Sovos' clients, Bellco Credit Union. Mr. Stadnik is very careful about sharing his sensitive PII. He stores any documents containing her PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. He would not have entrusted her PII to Sovo's client had he known of Sovos' lax data security policies. As a result of the Data Breach, and at the direction of Sovos' Notice, Mr. Stadnik made reasonable efforts to mitigate the impact of the Data Breach. He has spent significant time dealing with the

Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

19. Plaintiff Julianne Yenca is, and at all relevant times was, an individual citizen of the State of Arizona. She entrusted her PII to Defendant through her affiliation with one of Sovos' clients, Pacific Premier Bank. Ms. Yenca is very careful about sharing her sensitive PII. She stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. She would not have entrusted her PII to Sovo's client had she known of Sovos' lax data security policies. As a result of the Data Breach, and at the direction of Sovos' Notice, Ms. Yenca made reasonable efforts to mitigate the impact of the Data Breach. She has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

20. Plaintiff James Lawler is, and at all relevant times was, an individual citizen of the State of California. He entrusted his PII to Defendant through his affiliation with one of Sovos' clients, Patelco Credit Union. Mr. Lawler is very careful about sharing his sensitive PII. He stores any documents containing her PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. He would not have entrusted her PII to Sovo's client had he known of Sovos' lax data security policies. As a result of the Data Breach, and at the direction of Sovos' Notice, Mr. Lawler made reasonable efforts to mitigate the impact of the Data Breach. He has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

21. Plaintiff Tony Anderson is, and at all relevant times was, an individual citizen of the State of Indiana. He is unaware of how Sovos came into possession of his Private Information, but believes it was through one of his former credit unions or banks. Mr. Anderson is very careful about sharing his sensitive PII. He stores any documents containing her PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. He would not have entrusted her PII to Sovo's client had he known of Sovos' lax data security policies. As a result of the Data Breach, and at the direction of Sovos' Notice, Mr. Anderson made reasonable efforts to mitigate the impact of the Data Breach. He has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured. Additionally, Mr. Anderson was already harmed by the Data Breach in that a $3,500 loan taken out in his name soon after the Data Breach.

22. Sovos is a global digital regulatory compliance organization incorporated in Delaware, with its principal place of business at 200 Ballardvale Street, Building 1, 4th floor, Wilmington, Massachusetts 01887 in Middlesex County.

III. JURISDICTION AND VENUE

23. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Sovos. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has jurisdiction over Sovos because Sovos operates in this District.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District, and Sovos has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Sovos' Business and Collection of Plaintiffs' and Class Members' Private Information

26. Sovos is a digital regulatory compliance company. Founded in 1979, Sovos works in connection with its clients to regulate and maintain customer accounts. Upon information and belief, Sovos employs more than 2,600 people and generates approximately $504 million in annual revenue.

27. Sovos' clients, including the ones that provided services to the Plaintiffs and Class Members, purchased regulatory compliance solutions and services from Sovos.

28. Sovos' clients maintain PII for their own customers, which include Plaintiffs and Class Members.

29. As a condition of providing regulatory compliance services, Sovos requires that its clients entrust it with highly sensitive customer PII, including the Private Information belonging to Plaintiffs and Class Members.

30. In its "Privacy Policy," Sovos claims that "Protecting consumer privacy is important" and informs its clients and its clients' customers, who are Class Members, that:

> Sovos shall take reasonable steps to protect the Information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Sovos has put in place appropriate physical, electronic and managerial procedures to safeguard and secure the Information from loss, misuse, unauthorized access or disclosure, alteration or destruction.[2]

31. Sovos uses this information, *inter alia*, for marketing and sales purposes.

[2] *See* https://sovos.com/privacy-policy/ (last visited Dec, 1, 2023).

32. Because of the highly sensitive and personal nature of the information Sovos acquires and stores with respect to its clients' current and former customers. Sovos, upon information and belief, promises to, among other things: keep its clients' current and former customers' Private Information private; comply with industry standards related to data security and the maintenance of its clients' customers' Private Information; inform its clients (and their customers) of its legal duties relating to data security and comply with all federal and state laws protecting its clients' customers' Private Information; only use and release its clients' customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to its clients' customers if their Private Information is disclosed without authorization.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Sovos assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

34. Plaintiffs and Class Members relied on Sovos to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Sovos ultimately failed to do.

B. The Data Breach and Sovos' Inadequate Notice to Plaintiffs and Class Members

35. According to the Notice, Sovos learned of unauthorized access to its computer systems on May 31, 2023, with such unauthorized access having taken place on an undisclosed date(s). The Data Breach occurred because of vulnerabilities existing in the MOVEit file-transfer software Sovos used in the ordinary course of its business. The vulnerabilities allowed one or more unauthorized individuals to access the Private Information Sovos maintained for its clients, including the PII of Plaintiffs and Class Members.

36. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including Plaintiffs' and Class Members' Social Security numbers and account numbers.

37. On or about August 30, 2023, Sovos finally began to notify the majority of impacted individuals that its investigation determined their Private Information was compromised.

38. Sovos delivered the Notice to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "security event."

39. The Notice then attached additional pages that listed time-consuming steps victims of data security incidents can take to mitigate the inevitable negative impacts of the Data Breach on their lives, such as getting a copy of a credit report, reviewing account statements, placing freezes on their credit, and/or notifying law enforcement about suspicious financial account activity.

40. Other than offering to provide only two years of crediting monitoring that Plaintiffs and Class Members would have to affirmatively sign up for, along with a call center number victims could contact with questions, Sovos offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Sovos sent a similar generic Notice to all individuals affected by the Data Breach.

41. Sovos had obligations created by contract, industry standards, and common and statutory law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

42. Plaintiffs and Class Members provided their Private Information to Sovos' clients with the reasonable expectation and mutual understanding that Sovos would comply with its

obligations to keep such information confidential and secure from unauthorized access, and to provide timely notice of any security breach.

43. Sovos' data security obligations were particularly important given the substantial increase in cyberattacks in recent years. Sovos knew or should have known that its electronic records would be targeted by cybercriminals because of its regulatory compliance business that required Private Information to be provided to Sovos. However, even with these obligations and this knowledge, it failed to safeguard the Private Information.

44. Upon information and belief, the unencrypted PII of Class Members is for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

C. Sovos Failed to Comply with FTC Guidelines

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decisionmaking. Indeed, the FTC has concluded a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

46. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note businesses should protect the personal customer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer

networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

47. The FTC further recommends companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must reasonably take to meet their data security obligations.

49. As evidenced by the Data Breach, Sovos failed to properly implement basic data security practices. Sovos' failure to employ reasonable and appropriate measures to protect against unauthorized access to and exfiltration of Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

50. Sovos was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Sovos was also aware of the significant repercussions that would result from its failure to do so.

D. Sovos Failed to Comply with Industry Standards

51. As noted above, cybersecurity experts routinely identify businesses like Sovos as being particularly vulnerable to cyberattacks because of the value and volume of the Private Information which they collect and maintain.

52. Some industry best practices that should be implemented by these companies, including Sovos, are, without limitation: educating all employees and implementing strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, and multi-factor authentication, as well as backing up data and limiting which employees can access sensitive data.

53. As evidenced by the Data Breach, Sovos failed to follow some or all of these industry best practices.

54. Other best cybersecurity practices, standard in the industry, include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

55. As evidenced by the Data Breach, Sovos also failed to follow one or more of these cybersecurity best practices.

56. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

57. Sovos failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Sovos Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

58. In addition to its obligations under federal and state law, Sovos owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Sovos owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiffs and Class Members.

59. Sovos breached its obligations to Plaintiffs and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Sovos' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its clients' customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its clients' customers' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

60. Sovos negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

61. Had Sovos remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information in the Data Breach.

62. Accordingly, Plaintiffs' and Class Members' lives have been severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

F. Sovos Should Have Known that Cybercriminals Target Highly Sensitive PII to Carry Out Fraud and Identity Theft

63. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[3] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them

[3] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Dec, 1, 2023).

of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

64. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

65. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

66. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

67. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access

accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

68. For these reasons, the FTC recommends identity theft victims take several time-consuming steps (similar to those suggested by Sovos in its Notice) to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[4] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

69. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information to obtain fraudulent tax refunds. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

70. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

[4] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Dec. 1, 2023).

71. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[5] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Sovos' industry.

72. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports a stolen credit or debit card number can sell for $5 to $110 on the dark web and the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[7]

73. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to

[5] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military#:~:text=According%20to%20the%20nine%2Dcount,systems%20and%20commit%20economic%20espionage. (last visited on Dec. 1, 2023).

[6] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Dec. 1, 2023).

[7] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Dec. 1, 2023).

threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[8]

74. The Dark Web Price Index of 2022, published by PrivacyAffairs[9] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

75. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

76. Likewise, the value of PII is increasingly evident in our digital economy. Many companies collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and share it with third parties for similar purposes.[10]

77. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[11]

78. Consumers also recognize the value of their personal information, and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it.

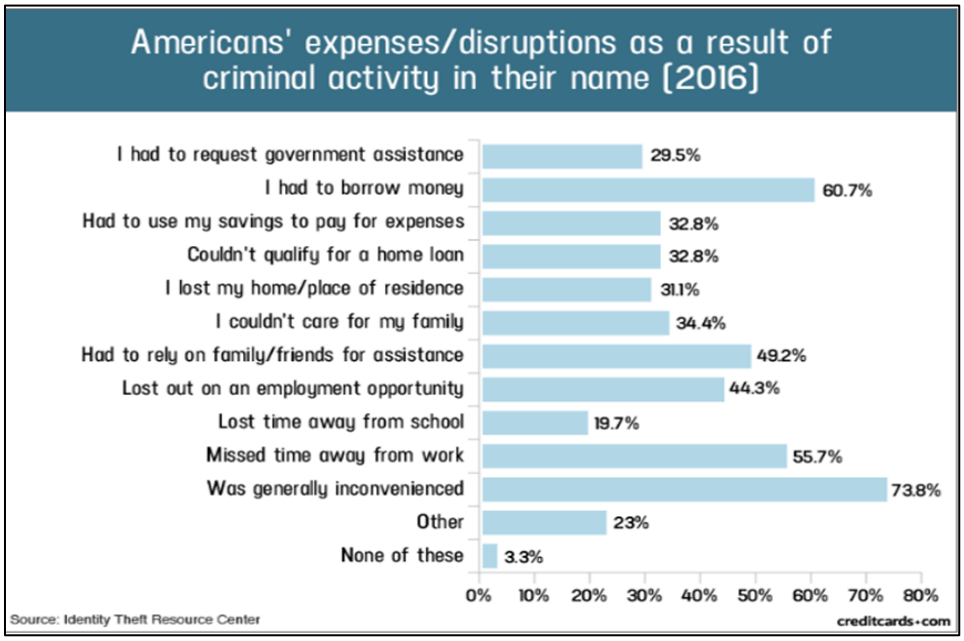
---

[8] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Dec. 1, 2023).
[9] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Dec. 1, 2023).
[10] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Dec. 1, 2023).
[11] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

79. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

80. Data breaches, like the one at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

81. A study by the Identity Theft Resource Center[12] shows the multitude of harms caused by fraudulent use of PII:



82. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information

[12] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Dec. 1, 2023).

is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[13]

> [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.

83. PII 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.

84. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiffs' and Class Members' Damages

85. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

86. As a direct and proximate result of Sovos' actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

87. In fact, such harm has already occurred in the case of Plaintiff Tony Anderson, who had a loan for $3,500 taken out in his name soon after the Data Breach.

88. Further, as a direct and proximate result of Sovos' conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

---

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Sept. 12, 2023).

89. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

90. The Private Information maintained by and stolen from Sovos' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can be and have been used to carry out these targeted fraudulent schemes against Plaintiffs and Class Members.

91. Additionally, Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their accounts and records for misuse.

92. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Placing "freezes" and "alerts" with credit reporting agencies;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

93. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Sovos, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

94. As a direct and proximate result of Sovos' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

95. Plaintiffs brings this action individually and on behalf of all other persons similar situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

96. Specifically, Plaintiffs propose the following "Nationwide Class" and "State Subclasses" (collectively referred to herein as the "Class" or "Classes"), subject to amendment as appropriate:

Nationwide Class

All living individuals in the United States who were sent a notice by Sovos or by a Sovos customer indicating that their Private Information was accessed in the Data Breach.

Arizona Subclass

All living individuals residing in Arizona who were sent a notice by Sovos or by a Sovos customer indicating that their Private Information was accessed in the Data Breach.

California Subclass

All living individuals residing in California who were sent a notice by Sovos or by a Sovos customer indicating that their Private Information was accessed in the Data Breach.

Indiana Subclass

All living individuals residing in Indiana who were sent a notice by Sovos or by a Sovos customer indicating that their Private Information was accessed in the Data Breach.

97. Excluded from the Classes are Sovos and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

98. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes, and to add other subclasses, before the Court determines whether certification is appropriate.

99. The proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

100. 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, based on information and belief, the Class consists of approximately 480,000 individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Sovos' records, Sovos' customers' records, Class Members' records, publication notice, self-identification, and other means.

101. Commonality. There are questions of law and fact common to the Classes which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Sovos engaged in the conduct alleged herein;

b. When Sovos learned of the Data Breach;

c. Whether Sovos' response to the Data Breach was adequate;

d. Whether Sovos unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether Sovos failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Sovos' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Sovos' data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Sovos owed a duty to Class Members to safeguard their Private Information;

i. Whether Sovos breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Sovos had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether Sovos breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether Sovos knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Sovos' misconduct;

o. Whether Sovos' conduct was negligent;

p. Whether Sovos' conduct was *per se* negligent;

q. Whether Sovos was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including declaratory relief, injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

102. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

103. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

104. Predominance. Sovos has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Sovos' conduct affecting Class Members set out above predominate

over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

105. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Sovos. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

106. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Sovos has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

107. Finally, all members of the proposed Class are readily ascertainable. Sovos, through its own records and those of its customers, has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Sovos.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

108. Plaintiffs restate and reallege all of the allegations in paragraphs 1-107 as if fully set forth herein.

109. Sovos knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

110. Sovos' duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

111. Sovos knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Sovos was on notice because, on information and belief, it knew or should have known it would be an attractive target for cyberattacks.

112. Sovos owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Sovos' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect its clients' customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

113. Sovos' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, 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 confidential data.

114. Sovos' duty also arose because Sovos was bound by industry standards to protect its clients' customers' confidential Private Information.

115. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on Sovos' part, and Sovos owed them a duty of care to not subject them to an unreasonable risk of harm.

116. Sovos, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within its possession.

117. Sovos, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

118. Sovos, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

119. Sovos breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. Sovos' specific negligent acts and omissions include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

120. Sovos acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

121. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices on the part of Sovos. Plaintiffs and Class Members had no ability to protect their Private Information that was in Sovos' possession. As such, a special relationship existed between Sovos and Plaintiffs and the Classes.

122. Only Sovos was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiffs and the Classes had entrusted to it.

123. Sovos' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

124. Sovos' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

125. As a result of Sovos' negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which third parties still possess, will be used for fraudulent purposes.

126. As a direct and proximate result of Sovos' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

127. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

128. Plaintiffs restate and reallege the allegations in paragraphs 1- 107 as if fully set forth herein.

129. Pursuant to Section 5 of the FTCA, Sovos had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

130. Sovos breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

131. Specifically, Sovos breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

132. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Sovos' duty in this regard.

133. Sovos also violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Classes and by not complying with applicable industry standards, as described herein.

134. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Sovos' networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

135. Plaintiffs and Class Members are within the class of persons that the FTCA are intended to protect and Sovos' failure to comply with both constitutes negligence *per se*.

136. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Sovos' negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

137. As a direct and proximate result of Sovos' negligence *per se*, Plaintiffs and the Class Members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

138. As a direct and proximate result of Sovos' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

139. Plaintiffs restate and reallege the allegations in paragraphs 1-107 as if fully set forth herein.

140. Sovos entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing regulatory compliance solutions and services. Upon information and belief, these contracts are virtually identical between and among Sovos and its clients around the country whose customers, including Plaintiffs and Class Members, were affected by the Data Breach.

141. In exchange, Sovos agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiffs and the Class Members.

142. These contracts were made expressly for the benefit of Plaintiffs and the Class Members, as Plaintiffs and Class Members were the intended third-party beneficiaries of the

contracts entered into between Sovos and its clients. Sovos knew that if it were to breach these contracts with its clients, the clients' customers—Plaintiffs and Class Members—would be harmed.

143. Sovos breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

144. Plaintiffs and the Class were harmed by Sovos' breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

145. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT/QUASI CONTRACT
(On behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

146. Plaintiffs restate and reallege the allegations in paragraphs 1-107 as if fully set forth herein.

147. This Count is pleaded in the alternative to Count III above because Plaintiffs and Class Members may not have an adequate remedy at law against Sovos, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

148. Plaintiffs and Class Members conferred a benefit on Sovos by turning over their Private Information to Sovos and utilizing its services directly or indirectly through their

relationships with one of Sovos' clients to whom Plaintiffs and Class Members entrusted their Private Information and who subsequently transmitted such Private Information to Sovos.

149. As a result of Sovos' clients' use of Sovos' services, Sovos received monetary benefits and the use of the valuable Private Information entrusted to it for business purposes and financial gain.

150. Sovos collected, maintained, and stored the Private Information of Plaintiffs and Class Members and, as such, had direct knowledge of the monetary benefits conferred upon it (including the use of the valuable Private Information for business purposes and financial gain) by Sovos' clients that collected Plaintiffs' and Class Members' Private Information and that used Sovos' services.

151. Sovos, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected Plaintiffs' and Class Members' Private Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiffs' and Class Members' Private Information.

152. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Private Information, Sovos, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class Members.

153. If Plaintiffs and Class Members had known that Sovos would not adequately secure their Private Information, they would not have agreed to provide such Private Information to Sovos.

154. Due to Sovos' conduct alleged herein, it would be unjust and inequitable under the circumstances for Sovos to be permitted to retain the benefit of its wrongful conduct.

155. As a direct and proximate result of Sovos' conduct, Plaintiffs and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (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 identity theft; (vi) the continued risk to their Private Information, which remains in Sovos' possession and is subject to further unauthorized disclosures so long as Sovos fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

156. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Sovos and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Sovos from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

COUNT V
VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
CAL BUS. & PROF. CODE § 17200, *ET SEQ.*
(On Behalf of Plaintiff Lawler and the California Subclass)

157. Plaintiff Lawler restates and realleges the allegations in paragraphs 1-107 as if fully set forth herein.

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

159. Sovos stored the Private Information of Plaintiff Lawler and California Subclass members in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept the Private Information of Plaintiff Lawler and the California Subclass members secure and prevented the loss or misuse thereof.

160. Plaintiff Lawler and the California Subclass were entitled to assume, and did assume, Sovos would take appropriate measures to keep their Private Information safe and secure.

161. Sovos did not disclose at any time that Private Information was vulnerable to hackers due to its data security measures being inadequate and/or outdated, and Sovos was in possession of that material information, which it had a duty to disclose.

162. Sovos violated the UCL by failing to maintain the safety and security of its computer systems.

163. Sovos violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted Privacy Policy, and by failing to immediately timely and adequately notify Plaintiff Lawler and California Subclass members of the Data Breach.

164. Section 5 of the FTCA required Sovos to take reasonable measures to protect the Private Information of Plaintiff Lawler and the California Subclass members and is a further source of Sovos' duty to Plaintiff Lawler and California Subclass members.

165. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Sovos of failing to implement and use reasonable measures to protect PII. Sovos, therefore, was required and obligated to take reasonable measures to protect the Private Information it solicited, possessed, held, or otherwise used.

166. The FTC publications and data security breach orders described herein further form the basis of Sovos' duty to adequately protect the Private Information. By failing to implement and use reasonable data security measures, Sovos acted in violation of Section 5 of the FTCA.

167. Sovos' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

168. If Sovos had complied with these legal requirements, Plaintiffs and California Subclass members would not have suffered the damages alleged herein related to the Data Breach, and consequently from, Sovos' failure to timely notify Plaintiff Lawler and California Subclass members of the Data Breach.

169. Moreover, Sovos' collection of the sensitive Private Information in combination with its failure to implement reasonable security safeguards demonstrate its violation of the unfair prong of the UCL.

170. Sovos violated the unfair prong of the UCL by establishing the sub-standard data security practices and procedures described herein; by soliciting and collecting the Private Information of Plaintiff Lawler and the California Subclass members with knowledge that it would

not be adequately protected; and by storing the Private Information of Plaintiff Lawler and the California Subclass members in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Lawler and California Subclass members. They were likely to deceive the public into believing their Private Information was securely stored when it was not. The harm these practices caused to Plaintiff Lawler and California Subclass members outweighed their utility, if any.

171. Plaintiff Lawler and California Subclass members, directly or indirectly, provided their Private Information to Sovos, which is property as defined by the UCL, and their property has been diminished in value as a result of the loss of its confidentiality.

172. Plaintiff Lawler and California Subclass members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Sovos' possession and is subject to further unauthorized disclosures so long as Sovos fails to undertake appropriate and adequate measures to protect the Private Information.

173. Unless restrained and enjoined, Sovos will continue to engage in the above-described wrongful conduct and more compromises of the Private Information it controls and maintains will occur.

174. As such, Plaintiff Lawler, on behalf of himself and the California Subclass, seeks restitution and an injunction, including public injunctive relief, prohibiting Sovos from continuing such wrongful conduct, and requiring Sovos to modify its corporate cultures and design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203.

175. To the extent any of these remedies are equitable, Plaintiff Lawler and the California Subclass seek such equitable remedies, in the alternative to any adequate remedy at law they may have.

COUNT VI
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 ("CCPA")
CAL. CIV. CODE § 1798, *ET SEQ.*
(On Behalf of Plaintiff Lawler and the California Subclass)

176. Plaintiff Lawler restates and realleges the allegations in paragraphs 1-107 as if fully set forth herein.

177. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure.

178. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction

of property, harassment, reputational damage, emotional stress, and even potential physical harm."[14]

179. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

180. Sovos failed to implement such procedures which resulted in the Data Breach.

181. CCPA also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party 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." Cal. Civ. Code § 1798.81.5(c).

182. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

183. Plaintiff Lawler and the California Subclass members are "consumer[s]" as defined by Cal. Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California

[14] *See* https://theccpa.org/ (last visited on December 1, 2023).

resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

184. Sovos is a "business" as defined by Cal. Civ. Code § 1798.140(c) because Sovos:

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

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

c. does business in California; and

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

185. The Private Information taken in the Data Breach is personal information as defined by Cal. Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff Lawler's, and California Subclass members', unencrypted first and last names and Social Security numbers, among other information.

186. Their Private Information was subject to unauthorized access and exfiltration, theft, or disclosure as it was wrongfully taken, accessed, and viewed by unauthorized third parties.

187. The Data Breach occurred as a result of Sovos' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect

the Private Information of Plaintiffs and California Subclass members. Sovos failed to implement reasonable data security procedures to prevent an attack on its server or network by hackers and to prevent unauthorized access of their Private Information as a result of this attack.

188. On December 1, 2023, Plaintiff Lawler provided Sovos with written notice of its violations of the CCPA, pursuant to Cal. Civil Code § 1798.150(b)(1), asserting violations of Cal. Civil Code §§ 1798.81.5 and 1798.150.

189. If Sovos has not cured or is unable to cure the violations described therein within thirty days of receipt, Plaintiff Lawler will amend his complaint to seek all relief available under the CCPA, including damages to be measured as the greater of actual damages or statutory damages in an amount up to $750.00 per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

190. As a result of Sovos' failure to implement and maintain reasonable data security procedures and practices that resulted in the Data Breach, Plaintiff Lawler and the California Subclass seek injunctive relief, including public injunctive relief and declaratory relief.

COUNT VII
VIOLATIONS OF ARIZONA CONSUMER FRAUD ACT
A.R.S. §§ 44-1521, *ET SEQ.*
(On Behalf of Plaintiffs Stadnik and Yenca and the Arizona Subclass)

191. Plaintiffs Stadnik and Yenca restate and reallege the allegations in paragraphs 1-107 as if fully set forth herein.

192. Sovos is a "person" as defined by A.R.S. § 44-1521(6).

193. Sovos advertised, offered or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

194. Sovos engaged in deceptive and unfair acts and practices, misrepresentation and the concealment, suppression and omission of material facts affecting the people of Arizona in

connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect the Private Information of Plaintiffs Stadnik and Yenca and Arizona Subclass members, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Stadnik and Yenca and Arizona Subclass members, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of the Private Information of Plaintiffs Stadnik and Yenca and Arizona Subclass members, 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 the Private Information of Plaintiffs Stadnik and Yenca and Arizona Subclass members, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*;

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure the Private Information of Plaintiffs Stadnik and Yenca and Arizona Subclass members; 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 the Private Information of Plaintiffs Stadnik and Yenca and Arizona Subclass members, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*

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

196. Sovos intended to mislead Plaintiffs Stadnik and Yenca and Arizona Subclass members and induce them to rely on its misrepresentations and omissions. Had Sovos disclosed to them that its data systems were not secure and, thus, vulnerable to attack, Sovos would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Sovos held itself out as a large, sophisticated entity with the resources to put adequate data security protocols in place, an organization that could be trusted with valuable PII regarding numerous consumers, including Plaintiffs Stadnik and Yenca and Arizona Subclass members. Sovos accepted the responsibility of hosting and keeping PII secure while keeping the inadequate state of its security controls secret from the public. Accordingly, because Sovos held itself out as having the ability to maintain a secure environment for PII with a corresponding duty of trustworthiness and care, Plaintiffs Stadnik and Yenca and Arizona Subclass members acted reasonably in relying on Sovos' misrepresentations and omissions, the truth of which they could not have discovered.

197. Sovos acted intentionally, knowingly and maliciously to violate Arizona's Consumer Fraud Act and recklessly disregarded the rights of Plaintiffs Stadnik and Yenca and Arizona Subclass members.

198. As a direct and proximate result of Sovos' unfair and deceptive acts and practices, Plaintiffs Stadnik and Yenca and Arizona Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PII.

199. Plaintiffs Stadnik and Yenca and Arizona Subclass members seek all monetary and nonmonetary relief allowed by law, including compensatory damages, disgorgement, punitive damages, injunctive relief and reasonable attorneys' fees and costs.

COUNT VIII
VIOLATIONS OF THE INDIANA DECEPTIVE CONSUMER SALES ACT
IND. CODE § 24-5-0.5 *ET SEQ*.
(On Behalf of Plaintiff Anderson and the Indiana Subclass)

200. Plaintiff Anderson restates and realleges the allegations in paragraphs 1-107 as if fully set forth herein.

201. Plaintiff Anderson the Indiana Subclass members, and Sovos each qualify as parties engaging in consumer transactions, as defined in Ind. Code § 24-5-0.5-2(a)(1).

202. As alleged herein in this Complaint, Sovos engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violations of the DCSA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Anderson's and Indiana Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

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

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Anderson's and Indiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that it would protect the privacy and confidentiality Plaintiff Anderson's and Indiana Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Anderson's and Indiana Subclass members' Private 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 Plaintiff Anderson's and Indiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Security breach.

203. Sovos' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Sovos' data security and ability to protect the confidentiality of consumers' Private Information.

204. In addition, Sovos' failure to secure Plaintiff Anderson's and Indiana Subclass members' Private Information violated the FTC Act and therefore violates the DCSA.

205. Sovos knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff Anderson's and Indiana Subclass members' Private Information, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

206. The aforesaid conduct violated the DCSA, Ind. Code § 24-5-0.5 et seq., in that it is a restraint on trade or commerce.

207. Sovos' violations of the DCSA have an impact of great and general importance to the public, including the people of Indiana. Thousands of Indiana residents have received services from Sovos, many of whom have been impacted by the Data Breach. In addition, Indiana residents have a strong interest in regulating the conduct of its health care services, whose policies described herein affect millions of people across the country.

208. As a direct and proximate result of Sovos' violation of the DCSA, Plaintiff Anderson's and Indiana Subclass members' Private Information are entitled to judgment under Ind. Code § 24-5-0.5, et seq., to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other further relief as the Court deems just and proper.

209. Sovos' implied and express representations that it would adequately safeguard Plaintiff Anderson's and Indiana Subclass members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Ind. Code § 24-5-0.5, et seq.

210. These violations have caused financial injury to Plaintiff Anderson's and Indiana Subclass members' and created an unreasonable, imminent risk of future injury.

211. Accordingly, Plaintiffs, on behalf of themselves and the Arizona Subclass members, bring this action under the DCSA to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT IX
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class)

212. Plaintiffs restate and reallege the allegations in paragraphs 1-107 as if fully set forth herein.

213. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the FTCA as described in this Complaint.

214. Sovos owes a duty of care to Plaintiffs and Class Members, which requires it to adequately secure Plaintiffs' and Class Members' Private Information.

215. Sovos still possesses Private Information pertaining to Plaintiffs and Class Members.

216. Plaintiffs and Class Members allege that Sovos' data security measures remain inadequate. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

217. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Sovos owes a legal duty to secure its customers' clients' Private Information under the common law and Section 5 of the FTCA;

b. Sovos' existing data security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect its customers' clients' Private Information; and

c. Sovos continues to breach this legal duty by failing to employ reasonable measures to secure its customers' clients' Private Information.

218. This Court should also issue corresponding prospective injunctive relief requiring Sovos to employ adequate security protocols consistent with legal and industry standards to protect its customers' clients' Private Information, including the following:

a. Order Sovos to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Sovos' explicit or implicit contractual obligations and duties of care, Sovos must implement and maintain reasonable security measures, including, but not limited to:

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

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

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

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Sovos' systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its customers' clients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

219. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Sovos. The risk of another such breach is real, immediate, and substantial. If another breach at Sovos occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

220. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Sovos if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Sovos' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Sovos has a pre-existing legal obligation to employ such measures.

221. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

Sovos, thus preventing future injury to Plaintiffs, Class Members, and others whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing Sovos to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Sovos to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: December 1, 2023

Respectfully submitted,

/s/ Christina Xenides

Christina Xenides (Bar No. 677603)
Mason A. Barney (*pro hac vice* submitted)*
Tyler J. Bean (*pro hac vice* submitted)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
cxenides@sirillp.com
mbarney@sirillp.com
tbean@sirillp.com

Jeff Ostrow (*Pro hac vice* submitted)*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Telephone: 954-525-4100
ostrow@kolawyers.com

Andrew J. Shamis (*Pro hac vice* forthcoming)
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 400
Miami, FL 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com

Counsel for Plaintiffs and the Putative Class

**Interim Co-Lead Counsel for Plaintiffs and the Putative Class*