UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVONNA JAMES, individually and on behalf of all others similarly situated, Plaintiff, v. COHNREZNICK LLP, Defendant.	Case No.: 1:21-cv-06544 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Davonna James ("Plaintiff") brings this Class Action Complaint against Defendant CohnReznick LLP ("Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. CohnReznick is a national professional services firm. Among other services, Defendant provides accounting and tax services to businesses.

2. On or about June 1, 2021, CohnReznick began notifying customers of Genesis Corp—one of businesses to which CohnReznick provides tax preparation services-- about a data breach that occurred sometime between February 26, 2021 and March 5,2021 (the "Data Breach").[1] Hackers obtained information from Defendant, including personally identifiable information ("PII")[2] of thousands of its clients' customers, including, but not limited to, their

[1] https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/Security-Breach-July2021.pdf (last visited July 19, 2021).

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

names and Social Security numbers.

3. Defendant claims on its website that it protects personal information: "CohnReznick will implement appropriate technical and organizational security measures designed to protect against the accidental loss, destruction, damage and/or unauthorized use of personal information."[3]

4. Not only did hackers steal the PII of Plaintiff and Class members, but, upon information and belief, criminals have already used the PII to attempt to steal some of Plaintiff's and Class members' identities. Hackers accessed and then either used or offered for sale the unencrypted, unredacted, stolen PII to criminals. This stolen PII has great value to hackers. Because of Defendant's Data Breach, customers' PII is still available and may be for sale on the dark web for criminals to access and abuse. Impacted consumers now face a present and certainly lifetime risk of identity theft.

5. As the National Director of Cybersecurity, Technology Risk, and Privacy Practice at CohnReznick acknowledged in a blog posted on February 23, 2021 to the CohnReznick website:

> Software supply chain attacks have increased significantly over the past few years. The overarching lesson to be learned from these incidents is that it's critical to fully understand the security of all of the third parties in your business ecosystem. Each partner represents an individual point of risk, and a breach of one can spread to other partners, vendors, and customers. Nonetheless, you own the risk and responsibility for protecting your assets, and it only takes one vendor breach to impact your business on a wide scale.[4]

6. Plaintiff's and Class members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and their failure to adequately protect the PII.

---

[3] *CohnReznick Client Data Privacy Notice*, CohnReznick (Feb. 28, 2020), https://www.cohnreznick.com/insights/client-data-privacy-notice (last visited July 19, 2021).

[4] Bhavesh Vadhani & Deborah Nitka, *SolarWinds breach underscores the need for monitoring third parties' security*, CohnReznick (Feb. 23, 2021), https://www.cohnreznick.com/insights/breach-underscores-need-to-monitor-third-parties-security (last visited July 19, 2021).

7. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect PII, (ii) warn its customers, potential customers, employees and other consumers of their inadequate information security practices, and (iii) effectively monitor their websites and platforms for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

8. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include, but are not limited to: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; and (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) deprivation of rights they possess under state consumer protection statutes.

PARTIES

9. Plaintiff Davonna James is a citizen of California residing in Merced, California.

10. Defendant CohnReznick is a limited liability partnership formed in New Jersey with its principal place of business in New York at 1301 Avenue of the Americas, New York, New York 10019.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant has its

principal place of business is located in the State of New York.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

14. Defendant is a professional services firm, including national accounting, tax, and business advisory services with offices across the United States and with subsidiaries around the globe. Defendant is one of the largest accounting, tax, and business advisory firms in the United States.[5]

15. In the ordinary course of doing business with Defendant, Defendant collects sensitive PII from consumers such as:

- Name;
- Address;
- Phone number;
- Driver's license number;
- Social Security number; and
- Date of birth.

16. In the course of collecting PII from consumers, including Plaintiff, Defendant promises to provide confidentiality and security for personal information, including by

[5] *Corporate Responsibility*, CohnReznick, https://www.cohnreznick.com/about (last visited July 19, 2021).

promulgating and placing privacy policies on its website.

17. Defendant promises that it will protect consumers' privacy and remain in compliance with statutory privacy requirements. For example, Defendant states on its website:

> CohnReznick will use commercially reasonable efforts to keep personal information confidential and to not disclose personal information to any third party except as permitted by the Contract, this Notice or with Client's prior written consent, except as stated herein. CohnReznick will implement appropriate technical and organizational security measures designed to protect against the accidental loss, destruction, damage and/or unauthorized use of personal information. CohnReznick will also enter into contracts with its Service Providers that require them to use commercially reasonable efforts to keep personal information confidential and implement appropriate security measures in connection with any processing of personal information performed on CohnReznick's behalf. CohnReznick will notify Client without undue delay after becoming aware of a breach of personal information as required by applicable law.[6]

18. Defendant, however, failed to protect and safeguard Plaintiff's and Class members' PII. In fact, there is no indication that Defendant followed even its most basic promises. For example, CohnReznick does not claim that any of the stolen PII was encrypted, including usernames and passwords.

The Data Breach

19. On or about June 1, 2021, Defendant began notifying consumers and state Attorneys General about a data breach that occurred between February 26, 2021 and March 5, 2021.

20. According to the Notice of Data Breach letters and letters sent to state Attorneys General, "an attachment document in an employee email account . . . was accessed by an unauthorized actor."

21. According to the Notice, Defendant thereafter "took steps to secure the account and

[6] *CohnReznick Privacy Notice*, *supra* note 3.

launched an investigation."

22. However, despite first learning of the Data Breach in February 2021 and concluding the investigation in May 2021, Defendant did not take any measures to notify affected Class members in a timely manner, waiting until on or about June 1, 2021

Defendant Was Aware of the Risks of a Data Breach

23. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and members of the Classes, to keep their PII confidential and to protect it from unauthorized access and disclosure.

24. Plaintiff and Class members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

26. Data breaches have become widespread. For example, the United States saw 1,244 data breaches in 2018 and had 446.5 million exposed records.[7] Defendant understood this reality because CohnReznick's Cybersecurity expert told consumers and businesses that the recent SolarWinds hack "amplif[ies] the need to fully understand your third-party landscape . . . because . . . fending off sophisticated threats will require that you understand the security controls deployed across your entire environment. We recommend a cybersecurity risk assessment to help you understand where critical data is located, how that data is classified, and who can access it."[8] However, as a third party to other businesses, CohnReznick failed to heed its own advice and

[7] Rob Sobers, *98 Must-Know Data Breach Statistics for 2021*, Varonis (Apr. 16, 2021), https://www.varonis.com/blog/data-breach-statistics (last visited July 19, 2021).

[8] *Solar Wind Breach*, *supra* note 4.

protect critical PII.

27. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

28. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[9] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[10]

29. The PII of Plaintiff and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

30. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and members of the Classes, including Social Security numbers, driver's license, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Classes a result of a breach.

---

[9] *See Taking Charge, What to Do If Your Identity is Stolen* at 3, Fed. Trade Comm'n (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited July 19, 2021).

[10] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *See Id.* at 3.

31. Plaintiff and members of the Classes now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

32. The injuries to Plaintiff and members of the Classes were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and members of the Classes.

Defendant Failed to Comply with FTC Guidelines

33. The 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 decision-making.

34. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that 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 that 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 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.

35. The FTC further recommends that 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security

measures.

36. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

38. Defendant was at all times fully aware of their obligation to protect the PII of customers, prospective customers and employees. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Failed to Comply with Industry Standards

39. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

40. Best cybersecurity practices that are standard in Defendant's industry include encrypting files; installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding

critical points.

41. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity 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 established standards in reasonable cybersecurity readiness.

42. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the Data Breach.

The Value of PII to Cyber Criminals

43. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

44. The PII of individuals 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, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11]

45. Social Security numbers, for example, are among the worst kind of personal

[11] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited July 19, 2021).

information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

46. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

47. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

48. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal

[12] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 19, 2021).
[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015, 4:59 AM), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 19, 2021).

> information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[14]

49. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and members of the Classes stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Classes. Stolen personal data of Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

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

51. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [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

[14] SSA, *Identity Theft and Your Social Security Number*, *supra* note 12.

from data breaches cannot necessarily rule out all future harm.[15]

52. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiff and members of the Classes has a high value on both legitimate and black markets.

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

54. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers and employees whose Social Security numbers have been compromised now face a present and imminent risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification

[15] *See* U.S. Gov't Accountability Off., GAO-07-737, *PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited July 19, 2021).

number, name, and date of birth.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

57. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

58. According to a recent article in the New York Times, cyber thieves are using driver's licenses obtained via insurance company application prefill processes to submit and fraudulently obtain unemployment benefits.[17] An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

The Plaintiff's Experience

Plaintiff Davonna James

59. Plaintiff James received the Notice of Data Breach from Defendant, dated June 1, 2021, on or about that date. The Notice informed Plaintiff that an "unauthorized actor" gained access to Plaintiff's full name and Social Security number when they breached Defendant's email

[16] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015, 5:49 AM), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 19, 2021).

[17] Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, New York Times (Apr. 27, 2021), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited July 19, 2021).

system.

60. As a direct and proximate result of the breach, Plaintiff James made reasonable efforts to mitigate the impact of the breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff James now reviews credit monitoring reports and/or checking account statements for irregularities two or three times per week, each time for approximately 5 minutes. This is valuable time Plaintiff James otherwise would have spent on other activities, including but not limited to work and/or recreation.

61. Plaintiff James is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

62. Plaintiff James suffered actual injury from having Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

63. Moreover, subsequent to the Data Breach, Plaintiff James also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls. Each day, Plaintiff James receives at least two scam phone calls, each of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

64. Plaintiff James has spent a significant amount of time since the Data Breach responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or

recreation.

65. As a result of the Data Breach, Plaintiff James anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff's and Class Member's Damages

66. To date, Defendant has done absolutely nothing to provide Plaintiff and Class members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach. What is more, Defendant places the burden squarely on Plaintiff and Class members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

CLASS ALLEGATIONS

67. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following Class:

> All natural persons residing in the United States whose PII was compromised in the Data Breach which occurred between February 26, 2021 and March 5, 2021 and announced on or about June 1, 2021 (the "Nationwide Class").

68. The California Subclass is defined as follows:

> All natural persons residing in California whose PII was compromised in the Data Breach which occurred between February 26, 2021 and March 5, 2021 and announced on or about June 1, 2021 (the "California Subclass").

69. The California Subclass is referred to herein as the "Statewide Subclass" and together with the Nationwide Class, are collectively referred to herein as the "Classes."

70. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

71. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

72. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

73. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiff and members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiff and members of the Classes;

f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep the PII of Plaintiff and members of the Classes secure and to prevent loss or misuse of that PII;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and members of the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Classes that their PII had been compromised;

j. Whether Defendant violated the consumer protection statutes invoked below; and

k. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief;

74. **Typicality**: Plaintiff's claims are typical of those of the other members of the Classes because all had their PII compromised as a result of the Data Breach due to Defendant's misfeasance.

75. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

76. **Superiority and Manageability**: Under Rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will

avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

77. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to the Subclass as a whole.

78. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

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

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

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF

Negligence
(On Behalf of Plaintiff, the Nationwide Class,
and the Statewide Subclass Against the Defendant)

79. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 78.

80. Defendant owed a common law duty to Plaintiff and members of the Classes to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

81. The legal duties owed by Defendant to Plaintiff and members of the Classes include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and members of the Classes in its possession;

b. To protect PII of Plaintiff and members of the Classes in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and members of the Classes of the Data Breach.

82. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the

Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

83. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and members of the Classes are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

84. Defendant breached its duties to Plaintiff and members of the Classes. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

85. Defendant knew or should have known that its security practices did not adequately safeguard the PII belonging to the Plaintiff and members of the Classes.

86. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiff and members of the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and members of the Classes during the period it was within Defendant's possession and control.

87. Defendant breached the duties it owes to Plaintiff and members of the Classes in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers and employees that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

88. Due to Defendant's conduct, Plaintiff and members of the Classes are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against Plaintiff and the members of the Classes.

89. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[18] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

90. As a result of Defendant's negligence, Plaintiff and members of the Classes suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the present and continued risk to their PII, which may remain for sale

[18] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and members of the Classes, including ongoing credit monitoring.

91. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the members of the Classes suffered was the direct and proximate result of Defendant's negligent conduct.

SECOND CLAIM FOR RELIEF

Negligence *Per Se*
(On Behalf of Plaintiff, the Nationwide Class, and the Statewide Subclass Against the Defendant)

92. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 78.

93. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

94. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including,

specifically, the immense damages that would result to Plaintiff and members of the Classes due to the valuable nature of the PII at issue in this case—including Social Security numbers.

95. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

96. Plaintiff and members of the Classes are within the class of persons that the FTC Act was intended to protect.

97. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Classes.

98. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the present and continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to

prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Classes.

99. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CLAIM FOR RELIEF

Violation of the California Consumer Privacy Act (On Behalf of Plaintiff and the Statewide Subclass Against the Defendant)

100. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 78.

101. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and members of the California Subclass's PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

102. The PII of Plaintiff and members of the California Subclass were subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant's violation of their duty under the CCPA.

103. Plaintiff and members of the California Subclass lost money or property, including but not limited to the loss of California Subclass members' legally protected interest in the

confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts described above.

104. Defendant knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII. As a result, the PII of Plaintiff and members of the California Subclass was exposed.

105. Defendant is organized for the profit or financial benefit of their owners and collects PII as defined in Cal. Civ. Code Section 1798.140.

106. Plaintiff and members of the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiff and members of the California Subclass. Plaintiff and members of the California Subclass have an interest in ensuring that their PII is reasonably protected.

107. On July 26, 2021 Plaintiff James's counsel sent a notice letter to Defendant's registered service agents via certified mail. Assuming Defendant does not cure the Data Breach within 30 days, and Plaintiff James believes any such cure is not possible under these facts and circumstances, Plaintiff James intends to promptly amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Class as authorized by the CCPA.

FOURTH CLAIM FOR RELIEF

Declaratory Judgment
(On Behalf of Plaintiff, the Nationwide Class,
and the Statewide Subclass Against the Defendant)

108. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 78.

109. Defendant owes a duty of care to Plaintiff and members of the Classes which requires Defendant to adequately secure PII.

110. Defendant still possess Plaintiff's and members of the Classes' PII.

111. Defendant does not specify in the Notice of Data Breach letter what steps they have taken to prevent this from occurring again.

112. Plaintiff and members of the Classes are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

113. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. 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 Defendant's systems;

e. Conducting regular database scanning and security checks;

f. 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;

g. Purchasing credit monitoring services for Plaintiff and members of the Classes for a period of ten years; and

h. Meaningfully educating Plaintiff and members of the Classes about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

FIFTH CLAIM FOR RELIEF

Unjust Enrichment
(On Behalf of Plaintiff, the Nationwide Class,
and the Statewide Subclass Against the Defendant)

114. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 78.

115. Defendant benefited from receiving Plaintiff's and members of the Classes' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

116. Defendant also understood and appreciated that Plaintiff's and members of the Classes' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

117. Plaintiff and members of the Classes who were customers of Defendant's customer conferred a monetary benefit upon Defendant in the form of monies paid for services available from Defendant.

118. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and members of the Classes. Defendant also benefited from the receipt of Plaintiff's and members of the Classes' PII, as Defendant used it to facilitate the transfer of PII between parties.

119. The monies that Plaintiff and members of the Classes paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

120. Defendant also understood and appreciated that Plaintiff's and members of the Classes' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

121. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and untrusted with Defendant. Indeed, if Defendant had informed Plaintiff and members of the Classes that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

122. As a result of Defendant's wrongful conduct, Defendant was unjustly enriched at the expense of, and to the detriment of, Plaintiff and members of the Classes. Defendant continues

to benefit and profit from their retention and use of the PII while its value to Plaintiff and members of the Classes has been diminished.

123. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiff's and members of the Classes' PII, while at the same time failing to maintain that information secured from intrusion and theft by hackers and identity thieves.

124. As a result of Defendant's conduct, Plaintiff and members of the Classes suffered actual damages in an amount equal to the difference in value between the amount Plaintiff and members of the Classes paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

125. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and members of the Classes paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

126. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Classes all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all members of the Classes, request judgment against the Defendant and that the Court grant the following:

A. An order certifying the Classes as defined herein, and appointing Plaintiff and their

counsel to represent the Classes;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and the members of the Classes;

C. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all members of the Classes;

D. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: August 2, 2021

Respectfully Submitted,

By: /s/ *Gary E. Mason*

Gary E. Mason (SBN 2163467)
David K. Lietz*
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Telephone: (202) 429-2290
Facsimile: (202) 429-2294
dlietz@masonllp.com
gmason@masonllp.com

M. Anderson Berry*
Alex Sauerwein*
CLAYEO C. ARNOLD,

A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
asauerwein@justice4you.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (202) 429-2290
Facsimile: (202) 429-2294
gklinger@masonllp.com

Attorneys for Plaintiff and the Classes

**Pro hac vice forthcoming*