UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

CHRISTOPHER HOFMANN, o*n behalf of himself and all others similarly situated,* Plaintiff, v. JERICO PICTURES, INC. d/b/a NATIONAL PUBLIC DATA, Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Christopher Hofmann ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Jerico Pictures, Inc. dba National Public Data ("NPD" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the data breach that upon information and belief occurred in or around April of 2024 involving Defendant NPD (the "Data Breach"), a background check company that allows its customers to search billions of records with instant results.[1]

2. Plaintiff brings this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices. Upon information and belief, such sensitive information includes, but is not limited to, Plaintiff's and Class Members' full names; current and past addresses (spanning

[1] *See* https://www.nationalpublicdata.com/about-us.html (last visited July 31, 2024).

at least the last three decades); Social Security numbers; information about parents, siblings, and other relatives (including some who have been deceased for nearly 20 years); and/or other personal information (collectively defined herein as "PII").

3. Upon information and belief, Defendant scrapes the PII of potentially billions of individuals from non-public sources.[2] Plaintiff and Class Members at no point knowingly provided their PII to Defendant and Defendant instead scraped their PII from non-public sources. To make matters even worse, Defendant did this without Plaintiff's and Class Members' consent or knowledge.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

II. PARTIES

5. Plaintiff Christopher Hofmann is and has been, at all relevant times, a resident and citizen of Fremont, California. On or about July 24, 2024, Plaintiff Hofmann received a notification from his identity theft protection service provider notifying him that his PII was compromised as a direct result of the "nationalpublicdata.com" breach, and that his PII had been found on the Dark Web. Plaintiff never provided Defendant with his PII and upon information and belief believes that his PII was scraped from non-public sources by Defendant. While Plaintiff Hofmann never directly provided his PII to Defendant, he never would have done so without the condition that it be maintained as confidential and with the understanding that Defendant would

[2] *See* Jessica Lyons, "Crooks threaten to leak 3B personal records 'stolen from background check firm'" *available at* https://www.theregister.com/2024/06/03/usdod_data_dump/ (last visited July 31, 2024).

employ reasonable safeguards to protect his PII. Plaintiff Hofmann never entrusted Defendant with his PII or allowed Defendant to maintain this sensitive PII.

6. Defendant Jerico Pictures Inc. dba National Public Data is a background check company with its headquarters located at 1801 NW 126th Way, Coral Springs, Florida 33071.

III. JURISDICTION AND VENUE

7. 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, including Plaintiff, are citizens of a state different from Defendant.

8. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

9. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

IV. FACTUAL BACKGROUND

Defendant's Business

10. Defendant Jerico Pictures, Inc. dba National Public Data ("NPD") is a background search company that "[m]any different businesses use [] to obtain criminal records, background checks and more all via XML integration."[3]

[3] *See supra* n.1.

11. Upon information and belief, Plaintiff and Class Members are not current and former customers but are individuals who had the misfortune of having their PII targeted, mined and scraped by Defendant from non-public sources without their consent.

12. Upon information and belief, Plaintiff's and Class Members' PII was entrusted to other unknown non-public sources and was then provided to Defendant by these sources for business purposes and for the benefit of Defendant and the unknown sources.

13. The information held by Defendant in their computer systems included the unencrypted PII of Plaintiff and Class Members.

14. Upon information and belief, Defendant made promises and representations to its customers, including the sources that held the PII of Plaintiff and Class Members and thereby Plaintiff and Class Members, that the PII collected from them as a condition of submitting a background check would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

15. Plaintiff and Class Members never provided their PII to Defendant. However, despite this fact, Plaintiff and Class Members still have the reasonable expectation and mutual understanding that Defendant, who used Plaintiff's and Class Members PII for its own business purposes, would comply with its obligations to keep such information confidential and secure from unauthorized access.

16. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant and upon information and belief its non-public clients to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized

disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

17. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

18. Defendant had obligations created by FTC Act, contract, industry standards, and upon information and belief representations made to its customers and thereby Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

19. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

20. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach

21. While no details have yet been revealed by Defendant as to how or when the data breach occurred, upon information and belief, a cybercriminal group by the name of USDoD gained access to Defendant's network prior to April 2024 and was able to exfiltrate the unencrypted PII of billions of individuals stored on Defendant's network (the "Data Breach"). Furthermore, upon information and belief, the PII was published, offered for sale and sold on the Dark Web by cybercriminals. Indeed, Plaintiff has already received notifications from his identity theft protection service that his PII was compromised and found on the Dark Web as a direct result of the "National Public Data" Data Breach.

22. On or about April 8, 2024, a criminal gang that goes by the name of USDoD posted a database entitled "National Public Data" on the Dark Web hacker forum named "Breached." USDoD alleged to have the PII of approximately 2.9 billion individuals and offered the database for purchase at a price of $3.5 million.[4] Specifically, VX-Underground, an educational website about malware and cyber security, reported the following:

> April 8th, 2024, a Threat Actor operating under the moniker "USDoD" placed a large database up for sale on Breached titled: "National Public Data". They claimed it contained 2,900,000,000 records on United States citizens. They put the data up for sale for $3,500,000.[5]

23. To make matters worse, VX-Underground reported that they "were informed USDoD intends on leaking the database" and that they "requested a copy in advance to confirm the validity of the data."[6] VX-Underground then "reviewed the massive file – 277.1GB uncompressed, and [] confirm[ed] the data present in it is real and accurate."[7] (Emphasis added).

24. VX-Underground also reported:

> 1. The database DOES NOT contain information from individuals who use data opt-out services. Every person who used some sort of data opt-out service was not present.
>
> 2. People who did not use data opt-out services and resided in the United States were immediately found. It showed their:
>
> - First name
> - Last name
> - Address
> - Address history (3 decades+)
> - Social security number
>
> It also allowed us to find their parents, and nearest siblings. We were able to identify someones parents, deceased relatives, Uncles, Aunts, and Cousins. Additionally,

[4] *See* https://x.com/vxunderground/status/1797047998481854512?s=46 (last visited July 31, 2024).
[5] *Id.*
[6] *Id.*
[7] *Id.*

> we can confirm this database also contains informed [sic] on individuals who are deceased. Some individuals located had been deceased for nearly 2 decades.[8]

25. Clearly, Defendant failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised, published, and then sold on the Dark Web, due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

26. Defendant has failed to provide Plaintiff and Class Members with timely and adequate notice including, but not limited to, information about how the Data Breach occurred and even when it occurred and when Plaintiff's and Class Members's information was released onto the Dark Web. Indeed, Defendant has still not provided any notice or warning to Plaintiff and Class Members. In fact, upon information and belief, the vast majority of Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

The Relief Plaintiff Seeks

27. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

[8] *Id*.

28. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromise, exfiltrated, published, and then sold to unknown criminals on the Dark Web. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

29. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) 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) remain backed up 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.

Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

Data Breaches Are Preventable.

30. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[9]

31. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

[9] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 31, 2024).

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[10]

32. To prevent and detect cyber-attacks NPD could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on

[10] *Id.* at 3-4.

any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[11].

33. To prevent and detect cyber-attacks or ransomware attacks NPD could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities

[11] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited July 31, 2024).

- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[12]

34. Given that Defendant was storing the sensitive PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

35. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of allegedly billions of individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores Plaintiff's and the Class's PII.

36. As part of its business practices, Defendant scrapes and/or acquires the sensitive PII of individuals, including Plaintiff and Class Members.

37. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its services.

[12] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited July 31, 2024).

38. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

41. Upon information and belief, Defendant made promises to its clients and thereby Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

42. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew, or Should Have Known, of the Risk Because Financing Companies in Possession of PII are Particularly Susceptible to Cyber Attacks.

43. Defendant’s data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

44. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

45. Data thieves regularly target companies like Defendant's due to the highly sensitive information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

46. Indeed, cyber-attacks, 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. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

47. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[14]

48. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[15]

---

[13]https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited July 31, 2024).

[14]*See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6 (last visited July 31, 2024).

[15] *Id*.

49. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

50. Additionally, as companies became more dependent on computer systems to run their business,[16] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[17]

51. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

52. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

53. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially billions of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[16]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited July 31, 2024).

[17] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited July 31, 2024).

54. To make matters worse, Defendant has not even provided any notice to any of the affected individuals whose PII was stolen in the Data Breach. This total failure to notice and a failure to compensate Plaintiff and Class Members. Moreover, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services in order to protect themselves from the consequences of Defendant's actions.

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

56. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

57. As a background search company in possession of individuals' sensitive PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] 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

[18] 17 C.F.R. § 248.201 (2013).

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."[19]

59. 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.[20] For example, Personal Information can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

60. For example, Social Security numbers are among the worst kind of PII 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 stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, 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

---

[19] *Id.*

[20] *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 July 31, 2024).

[21] *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 July 31, 2024).

[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 31, 2024).

> illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

61. What's 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.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he 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."[24]

63. 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 and name.

64. 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,

---

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 31, 2024).

[24] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 31, 2024).

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[25]

65. 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.

66. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

67. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

Defendant Fails to Comply with FTC Guidelines.

68. 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 decision-making.

---

[25] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 31, 2024).

[26] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited July 31, 2024).

69. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These 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.[27]

70. 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.[28]

71. 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.

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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

---

[27] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 31, 2024).

[28] *Id.*

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. These FTC enforcement actions include actions against financial companies, like Defendant. *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 408 (E.D. Va. 2020) *("*"Plaintiffs have plausibly alleged a claim" based upon violation of Section 5 of the FTC Act.)

74. Section 5 of the FTC Act, 15 U.S.C. § 45, 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, 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.

75. Defendant failed to properly implement basic data security practices.

76. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

77. Upon information and belief, NPD was at all times fully aware of its obligation to protect the PII of its Plaintiff and Class Members, NPD was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails to Comply with Industry Standards.

78. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

79. Several best practices have been identified that, at a minimum, should be implemented by financial companies in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. NPD failed to follow these industry best practices, including a failure to implement multi-factor authentication.

80. Other best cybersecurity practices that are standard in Defendant's industry include 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; training staff regarding critical points. NPD failed to follow these cybersecurity best practices, including failure to train staff.

81. 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.

82. These frameworks are existing and applicable industry standards in Defendant's industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, opening the door to the threat actors and causing the Data Breach.

Common Injuries and Damages

83. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as NPD fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

Data Breaches Increase Victims' Risk of Identity Theft.

84. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers. Indeed Plaintiff has already been alerted that his PII has been found on the Dark Web.

85. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

86. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the

data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

87. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

88. As a result of the recognized risk of identity theft, when a Data Breach occurs, and assuming an individual is notified by a company that their PII was compromised, which Defendant has failed to do in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

89. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

90. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as monitoring their credit and reviewing their financial accounts for any indication of fraudulent activity, which may take years to detect.

91. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[29]

92. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[30]

93. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

Diminution Of Value Of PII

94. PII is a valuable property right.[31] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

[29] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited July 31, 2024).

[30] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 31, 2024).

[31] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited July 31, 2024) ("GAO Report").

95. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[32]

96. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[33] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[34,35]

97. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available on the Dark Web, and the rarity of the Data has been lost, thereby causing additional loss of value.

98. At all relevant times, NPD knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[32] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[33] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 31, 2024).

[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 31, 2024)

[35] https://datacoup.com/ (last visited July 31, 2024).

99. The fraudulent activity resulting from the Data Breach may not come to light for years.

100. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

101. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially billions of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary

103. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

104. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

105. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

106. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of Benefit Of The Bargain

107. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. Upon information and belief, when agreeing to pay Defendant's clients for services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII, when in fact, NPD did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant's clients, and thereby Defendant.

Plaintiff Christopher Hofmann's Experience

108. Plaintiff's personal identification information, including but not limited to, his Social Security number, was in the possession, custody and/or control of Defendant at the time of the Data Breach.

109. Plaintiff believed that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or

disclosure, and would timely notify him of any data security incidents related to him. Plaintiff would not have permitted his PII to be given to Defendant had he known it would not take reasonable steps to safeguard his PII.

110. On or around late July 2024, Plaintiff received notice from Experian that his PII, including his Social Security number, is being sold on the Dark Web after a breach involving Defendant and/or Defendant's website, www.nationalpublicdata.com.

111. As a result of the Data Breach, Plaintiff has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

112. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; (c) the theft of his PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

113. As a result of the Data Breach, Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

114. The Data Breach has caused Plaintiff to suffer significant anxiety and stress, which has been compounded by the fact that his Social Security number and other intimate details are in the hands of criminals and being sold on the Dark Web.

115. As a result of the Data Breach, Plaintiff anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of

identity theft and fraud for his lifetime.

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

V. CLASS ACTION ALLEGATIONS

117. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

118. The Classes that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach (the "Nationwide Class").
>
> All individuals residing in California whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach (the "California Subclass") (collectively with the Nationwide Class, the "Class" unless otherwise specified).

119. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; 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, as well as their immediate family members.

120. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

121. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. On information and belief potentially billions of individuals will soon be notified by Defendant of the Breach. The Class is apparently identifiable

within Defendant's records, and Defendant has already identified these individuals or is in the process of doing so (as evidenced by sending them breach notification letters).

122. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. 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;

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

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

123. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

124. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

125. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

126. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

127. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff wase exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

128. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

129. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

130. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

131. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

132. Likewise, particular issues under Rule 42(d)(1) 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 failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

133. Plaintiff repeats and re-alleges paragraphs 1-133 in the Complaint as if fully set forth herein.

134. Defendant, upon information and belief, scrapes the sensitive PII of individuals, including Plaintiff and Class Members, in the ordinary course of providing background check services to its clients. Furthermore, upon information and belief, Defendant scrapes the PII of individuals from non-public sources including but not limited to its clients.

135. Upon information and belief, Plaintiff and Class Members entrusted Defendant's non-public clients with their PII and Defendant scraped and then stored this PII for the purpose of making money by providing background check services.

136. NPD owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

137. NPD had a duty to employ reasonable security measures 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.

138. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between NPD and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted NPD's clients, and thereby NPD, with their confidential PII.

139. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because NPD is bound by industry standards to protect confidential PII.

140. NPD was subject to an "independent duty," untethered to any contract between NPD and Plaintiff or the Class.

141. NPD also had a duty to exercise appropriate clearinghouse practices to remove individuals' PII it was no longer required to retain pursuant to regulations.

142. NPD also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

143. NPD breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by NPD include, but are not limited to, the following:

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

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

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

144. NPD violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

145. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

146. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

147. Defendant's violation of the FTC Act is prima facie evidence of negligence.

148. 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 their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

149. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

150. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

151. NPD has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

152. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. NPD knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

153. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

154. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

155. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

156. NPD had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

157. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

158. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

159. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) 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) remain backed up 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.

160. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

161. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as NPD fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

162. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

163. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

164. Plaintiff and Class Members are also entitled to injunctive relief requiring NPD to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

165. Plaintiff repeats and re-alleges paragraphs 1-133 in the Complaint as if fully set forth herein.

166. Upon information and belief, Plaintiff and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current customers, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

167. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (all customers entering into the contracts), as Defendant's service was for background check services for Plaintiff and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these services.

168. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

169. Defendant materially breached its contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

170. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

171. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

172. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

173. Plaintiff repeats and re-alleges paragraphs 1-133 in the Complaint as if fully set forth herein.

174. This count is pleaded in the alternative to the breach of third-party beneficiary contract count above (Count II).

175. Plaintiff and Class Members conferred a monetary benefit to Defendant when they provided their PII and payment to Defendant's clients who used Defendant's background check services.

176. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant's customers, and thereby Defendant, and it accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of Plaintiff and Class Members PII to Defendant from its clients is an integral part of Defendant's business. Without collecting and maintaining Plaintiff's and Class Members' PII, Defendant would be unable to offer background check services.

177. Defendant was supposed to use some of the monetary benefit provided to it by its clients at Plaintiff's and Class Members' expense to secure the PII belonging to Plaintiff and Class Members by paying for costs of adequate data management and security.

178. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement necessary security measures to protect the PII of Plaintiff and Class Members.

179. Defendant gained access to the Plaintiff's and Class Members' PII through inequitable means because Defendant failed to disclose that it used inadequate security measures.

180. Plaintiff and Class Members were unaware of the inadequate security measures and would not have entrusted their PII to Defendant's clients, and thereby Defendant, had they known of the inadequate security measures.

181. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

182. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv)

loss of benefit of the bargain; and (v) 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) remain backed up 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.

183. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

184. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds from the monetary benefit that it unjustly received from them.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

185. Plaintiff repeats and re-alleges paragraphs 1-133 in the Complaint as if fully set forth herein.

186. In providing their PII to Defendant's clients and thereby Defendant, Plaintiff and Class Members justifiably placed a special confidence in Defendant and its clients to act in good faith and with due regard for the interests of Plaintiff and Class Members to safeguard and keep confidential that PII.

187. Defendant accepted the special confidence Plaintiff and Class Members placed in it.

188. In light of the special relationship between NPD and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' PII, Defendant became

a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its clients and the customers of its clients, including Plaintiff and Class Members, for the safeguarding of Plaintiff's and Class Members' PII.

189. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its customer relationships, in particular, to keep secure the PII of its clients' customers.

190. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect the integrity of the systems containing Plaintiff's and Class Members' PII.

191. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

192. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) 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; (v) the 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 in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of the services they paid for and received.

193. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm and other economic or non-economic loss.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

194. Plaintiff repeats and re-alleges paragraphs 1-133 in the Complaint as if fully set forth herein.

195. 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 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

196. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether NPD is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that NPD's data security measures remain inadequate. Furthermore, Plaintiff continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in future.

197. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. NPD owes a legal duty to secure patients' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTCA; and

b. NPD continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII.

198. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at NPD. The risk of another such breach is real, immediate, and substantial. If another breach at NPD occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and he will be forced to bring multiple lawsuits to rectify the same conduct.

199. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to NPD if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to NPD of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and NPD has a pre-existing legal obligation to employ such measures.

200. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at NPD, thus eliminating the additional injuries that would result to Plaintiff and other individuals whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

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

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

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

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

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

Vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

x. requiring Defendant to conduct regular database scanning and securing checks;

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

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

xiii. requiring Defendant to implement a system of tests to assess its

employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: August 1, 2024

Respectfully Submitted,

/s/ Jeff Ostrow
Jeff Ostrow FBN 121452
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
ostrow@kolawyers.com

M. Anderson Berry*
Gregory Haroutunian*
Brandon P. Jack*
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Tel: (916) 239-4778
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Jason M. Wucetich*
WUCETICH & KOROVILAS LLP
222 North Sepulveda Boulevard, Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201
jason@wukolaw.com

**Pro Hac Vice Forthcoming*

Attorneys for Plaintiff and the Putative Class