BRADLEY/GROMBACHER, LLP
Kiley Grombacher, Esq. (SBN 245960)
31365 Oak Crest Drive, Suite 240
Westlake Village, CA 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
Email: kgrombacher@bradleygrombacher.com

Attorneys for Plaintiff CHARLES J. GELETKO
on behalf of himself and others similarly situated

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

CHARLES J. GELETKO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

JERICO PICTURES, INC., d/b/a NATIONAL PUBLIC DATA

Defendant.

CASE NO.

CLASS ACTION

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE/NEGLIGENCE *PER SE*;**
2. **UNJUST ENRICHMENT;**
3. **INVASION OF PRIVACY;**
4. **BREACH OF THIRD-PARTY BENEFICIARY CONTRACT;**
5. **BREACH OF IMPLIED CONTRACT;**
6. **CALIFORNIA'S CONSTITUTIONAL RIGHT TO PRIVACY;**
7. **CALIFORNIA CONSUMER LEGAL REMEDIES ACT; AND**
8. **CALIFORNIA'S UNFAIR COMPETITION LAW, CALIFORNIA BUS. & PROF. CODE § 17200, ET SEQ.**

JURY TRIAL DEMANDED

Plaintiff Charles J. Geletko, ("Plaintiff") bring this Class Action Complaint against Defendant Jerico Pictures, Inc., d/b/a National Public Data ("Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

STATEMENT OF FACTS

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII") of roughly 2 billion people, including, but not limited to: full name, date of birth, address, phone number, Social Security Number, and other information regarding relatives.

2. Using the above personal information, it is possible to identify an individual's parents, nearest siblings, uncles, aunts, cousins, and deceased relatives—including individuals who have been deceased for nearly twenty years.[1]

3. Upon information and belief, Defendant collects and sells access to personal data for use in background checks, private investigations, mobile applications, and by data resellers.[2] The data Defendant collects is scraped from public and/or non-public sources, without the data subject's knowledge or consent, and is compiled into individual profiles. A major problem with this practice is that Defendant has no ties with the data subjects, so most of them will have no idea that their data has been disclosed without their authorization.

4. In, or around, April 2024, a cybercriminal called "USDoD" claimed to have access to almost 2.7 billion records of personal information that was obtained from National Public Data databases and subsequently leaked the data on a hacking

[1] https://x.com/vxunderground/status/1797047998481854512?s=46

[2] https://www.nationalpublicdata.com/

forum (hereafter referred to as the "Data Breach"). "Since then, various threat actors have released partial copies of the data, with each leak sharing a different number of records and, in some cases, different data."[3]

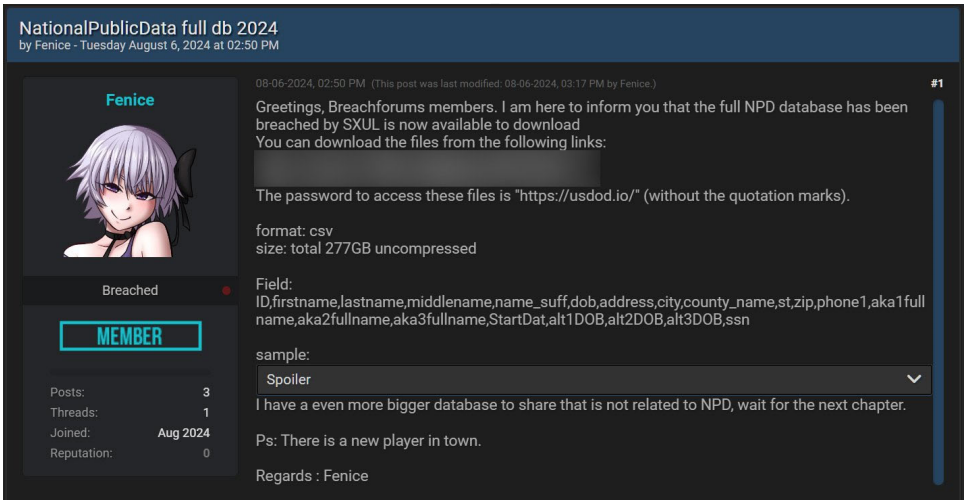

**Image from a threat actor known as "Fenice" leaking the National Public Data on a hacking forum*

5. "The value of the National Public Data records from a criminal's perspective comes from the fact that they have been collected and organized. While the information is largely already available to attackers, they would have had to go to great lengths at great expense to put together a similar collection of data, so essentially [National Public Data] just did them a favor by making it easier." Furthermore, since the data set contains records regarding deceased persons, criminals can use the data "to create birth certificates, voting certificates, etc., that will be valid."[4]

6. To date, Defendant has failed to send data breach notice letters to individuals who were affected by the Data Breach discussing the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures

[3] https://www.bleepingcomputer.com/news/security/hackers-leak-27-billion-data-records-with-social-security-numbers/

[4] https://www.techrepublic.com/article/social-security-numbers-leak/

undertaken to ensure such a breach does not occur again. These details have not been explained or clarified to Plaintiff, who retain a vested interest in ensuring that their PII remains protected.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

8. The Data Breach was a direct result of Defendant's failure to implement reasonable safeguards to protect PII from a foreseeable and preventable risk of unauthorized disclosure. Had Defendant implemented administrative, technical, and physical controls consistent with industry standards and best practices, it could have prevented the Data Breach.

9. Defendant's conduct resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals. The unauthorized disclosure of Plaintiff's PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff.

10. More specifically, Defendant is a data aggregator that collects and sells personal data that it gathers from various data broker websites. As a result of Defendant's failure to protect Plaintiff's PII, Plaintiff is now required to spend time and money finding and removing data from data broker websites. The data removal process involves:

a. Scanning data broker websites to find records.[5]
b. Performing "opt-outs" on each data broker website.
c. Confirming the data removal request by email.
d. Submitting completed PDF forms.

[5] A list of the numerous data broker websites can be found here: https://privacyrights.org/data-brokers

e. Receiving confirmation codes and submitting them to the data broker websites.

f. Continued scanning of the data broker websites to confirm removal of PII.

g. Regularly scheduling monitoring of all data broker websites to detect reappearing records.

11. The cost to automate this "opt-out" process is $355.32 a year or $32.90 per month.[6] The necessary time and/or money spent finding and removing data from data broker websites is an actual, particularized, and concrete harm, traceable to the Defendant's failure to adequately secure the PII in its custody. The harm suffered, as described herein, can be redressed by a decision awarding Plaintiff and Class Members monetary damages in this matter.

12. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

13. Defendant's conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft, fraud, or other forms of exploitation. The circumstances demonstrating a substantial risk of future exploitation include, but are not limited to:

a. **Sensitive Data Type**: The data acquired in the Data Breach included unencrypted social security numbers, dates of birth, full names, addresses, and phone numbers. Upon information and belief, this category of data is used by cybercriminals to perpetuate fraud, identity theft, and other forms of exploitation.[7]

---

[6] The annual plan reflects a 10% discount. *See,* IDX, Individual Consumer Plans, https://www.idx.us/privacy-identity-protection/consumer-plans (last access August 13, 2024).

[7] https://www.f-secure.com/us-en/articles/why-do-hackers-want-your-personal-information

b. **Data Breach Type**: USDoD, the cybercriminal initially posting the stolen data for sale has a history of using information stealing trojans like RedLine. "Info-stealers like RedLine typically are deployed via email malware campaigns, and by secretly bundling the trojans with cracked versions of popular software titles made available online. Credentials stolen by info-stealers often end up for sale on cybercrime shops that peddle purloined passwords and authentication cookies."[8]

c. **Data Misuse**: Upon information and belief, USDoD obtained the database from another threat actor using the alias "SXUL." Since April 2024, various threat actors have released partial copies of the data acquired in the Data Breach on the dark web.[9] The dark web uses a series of encrypted networks to hide users' identities, which makes it convenient for criminals to buy and sell illegally obtained data. Many criminals purchase stolen personal data off the dark web before launching social engineering-based attacks. A social engineering attack is a method of using psychological manipulation to deceive a victim and gain access to a computer system or to steal sensitive information such as login credentials. Social engineering attacks that can be launched using names, telephone numbers and email addresses include phishing, smishing (SMS message), vishing (voice messaging), pretexting, and baiting attacks.

14. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PII in its custody, and has created a separate, particularized, and concrete harm to Plaintiff.

15. More specifically, Plaintiff's exposure to the substantial risk of future exploitation caused them to: (i) spend money on mitigation measures like credit monitoring services and/or dark web searches; (ii) lose time and effort spent responding to the Data Breach or removing their data from data broker websites; and/or (iii) experience emotional distress associated with reviewing accounts for

[8] https://krebsonsecurity.com/2023/09/fbi-hacker-dropped-stolen-airbus-data-on-9-11/

[9] https://www.bleepingcomputer.com/news/security/hackers-leak-27-billion-data-records-with-social-security-numbers/

fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff suffered can be redressed by a favorable decision in this matter.

16. Plaintiff faces a substantial risk of future spam, phishing, or other social engineering attacks where their full names, addresses, and phone numbers were stolen by a cybercriminal, known for stealing and reselling personal data on the dark web. Names, telephone numbers and email addresses can be used by cybercriminals to launch social engineering attacks designed to trick individuals into giving away sensitive information.

17. Armed with the PII acquired in the Data Breach, data thieves have already engaged in theft and can, in the future, commit a variety of crimes including, opening new financial accounts, taking out loans, using Class Members' PII to obtain government benefits, file fraudulent tax returns, obtain driver's licenses, and give false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff has suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

19. Defendant, as a data collector and/or data aggregator, was obligated to use reasonable technical, administrative, and physical safeguards to protect the PII in its possession.

20. Plaintiff was unaware that Defendant was collecting, aggregating, and selling their PII and thus relied on this sophisticated business entity to keep their PII confidential and securely maintained.

21. Plaintiff and Class Members were impacted by the Data Breach. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate data protection practices and for failing to provide timely and adequate notice of the Data Breach.

22. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff has a continuing interest in ensuring that personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

Data Breaches Are Avoidable

23. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

24. Upon information and belief, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) implement reasonable data protection measures for the collection, use, disclosure, and storage of personal information; and/or (iii) ensure its third-party vendors were required to implement reasonable data protection measures.

25. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to

restore control over the network.[10] Ransomware groups frequently implement a double extortion tactic, "where the cybercriminal posts portions of the data to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[11]

26. Upon information and belief, the Data Breach also occurred as a result of a phishing attack. A phishing attack involves the use of fraudulent emails, social media messages, text messages, websites, or other communication to trick people into revealing login credentials or other sensitive information. Phishing attacks are prevalent because they exploit human vulnerabilities. Cybercriminals can use phishing attacks to "trick people who have authorized access to their target—be it money, sensitive information or something else—into doing their dirty work."[12]

27. To detect and prevent cyber-attacks, Defendant could and should have implemented the following measures:

Reasonable Safeguards

a. Regularly patch critical vulnerabilities in operating systems, software, and firmware on devices. Consider using a centralized patch management system.

b. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.

---

[10] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs

[11] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[12] *What is phishing?* IBM security topics, https://www.ibm.com/topics/phishing (accessed August 14, 2024).

c. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

d. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

e. 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.

f. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

g. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

h. Configure firewalls to block access to known malicious IP addresses.

i. Set anti-virus and anti-malware programs to conduct regular scans automatically.

j. 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.

k. 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.

l. 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.

m. 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.

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

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

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

q. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

r. Conduct an annual penetration test and vulnerability assessment.

s. Secure your backups.[13]

t. Identify the computers or servers where sensitive personal information is stored.

u. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

v. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

w. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

x. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

y. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

---

[13] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

z. To detect network breaches when they occur, consider using an intrusion detection system.

aa. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

bb. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

cc. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

dd. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[14]

28. Given that Defendant collected, used, and stored PII, Defendant could and should have identified the risks and potential effects of collecting, maintaining, and sharing personal information.

29. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. 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 Plaintiff's and the Class Members' PII.

30. Defendant knew and understood unencrypted PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant

---

[14] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and Class Members as a result.

Plaintiff and Class Members Have Sustained Damages in the Data Breach

31. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct. As a consequence of the Data Breach, Plaintiff and Class Members sustained monetary damages that exceed the sum or value of $5,000,000.00.

32. As a result of Defendant's failure to protect Plaintiff's PII, Plaintiff is now required to spend time and money finding and removing data from data broker websites. Notably, the database of information involved in the Data Breach does not contain information from individuals who previously used data opt-out services.[15]

33. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft, fraud, or other exploitation where their names, social security numbers, and dates of birth were targeted by a sophisticated hacker known for stealing and reselling sensitive data on the dark web. The substantial risk of future identity theft and fraud created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

34. Furthermore, Plaintiff and Class Members face a substantial risk of future spam, phishing, or other attacks designed to trick them into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime, where their names and contact information were acquired in the Data Breach and subsequently released on the dark web. The substantial risk of future exploitation

[15] *See*, https://x.com/vxunderground/status/1797047998481854512?s=46

created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

35. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[16] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

36. Given the type of targeted attack in this case, the sophistication of the criminal posting about the data acquired in the Data Breach, the type of PII involved in the Data Breach, the hacker's behavior in prior data breaches, the ability of criminals to link data acquired in the Data Breach with information available from other sources, and the fact that the stolen information has been placed on the dark web, it is reasonable for Plaintiff and Class Members to assume that their PII was obtained by, or released to, criminals intending to utilize the PII for future identity theft-related crimes or exploitation attempts.

37. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional

---

[16] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package typically includes the victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm

time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach, including opting-out of data broker websites.

38. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) 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); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[17]

39. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year. As mentioned above, the cost to automate the "opt-out" process is between $355.32 and $394.80 a year to have data removed from data broker websites.

40. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and illegitimate markets, has been damaged and diminished by its 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, and the rarity of the data has been lost, thereby causing additional loss of value.

---

[17] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

41. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[18] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[19] Sensitive PII can sell for as much as $363 per record.[20]

42. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By collecting Plaintiff's and Class Members' PII, using their PII for profit or to improve the ability to make profits, and then permitting the unauthorized disclosure of the PII, Plaintiff and Class Members were deprived of the benefit of their bargain.

43. By selling products or services that disclosed Plaintiff's and Class Members' PII, Defendant undertook a duty to protect their personal data. However, Defendant did not invest the funds into implementing reasonable data security practices.

44. Through this Complaint, Plaintiff seeks redress individually, and on behalf of all similarly situated individuals, for the damages that resulted from the Data Breach.

JURISDICTION & VENUE

45. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332(d), because this is a class action wherein the amount in controversy exceeds the sum or value of

---

[18] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[19] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[20] *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).

$5,000,000.00, 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 each Defendant.

46. Defendant is subject to personal jurisdiction in this district because it has substantial aggregate contacts throughout the United States and the state of California. Defendant has engaged, and continue to engage, in conduct that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, and the state of California, and this District, and it purposely availed itself of the laws of the United States and the State of California.

47. Defendant is subject to personal jurisdiction in this District because it purposely avails itself of the privilege of conducting activities in the United States and the State of California and directs business activities toward consumers throughout the United States and the State of California. Furthermore, Defendant engaged and continues to engage in conduct that has a foreseeable, substantial effect throughout the United States, the State of California, and this District connected with its unlawful acts.

48. Venue is proper in this District under 28 U.S.C §1391(b) because Plaintiff and thousands of potential Class Members reside in this District; Defendant transacts business in this District; and Defendant intentionally avails itself of the laws within this District.

PARTIES

49. Plaintiff Charles J. Geletko is a citizen of the State of California. At all relevant times, Plaintiff has been a resident of Burbank, California. Plaintiff's data was compromised as a direct result of the Data Breach.

50. Defendant Jerico Pictures Incorporated, d/b/a National Public Data is a Florida corporation with its principal place of business at 1801 N.W. 126th Way, Coral Springs, Broward County, Florida 33071. Defendant's registered agent for

service of process is Verini Salvatore Jr., 1801 N.W. 126th Way, Coral Springs, Broward County, Florida 33071.

CLASS ALLEGATIONS

51. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

52. The Classes that Plaintiff seeks to represent are defined as follows:

Nationwide Class

All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach that occurred in, or around, April 2024 (the "Class").

Dark Web Monitoring Subclass

All individuals residing in the United States who were notified by a dark web monitoring and identity protection service that their PII was accessed and acquired by an unauthorized party as a result of National Public Data's, Data Breach that occurred in, or around, April 2024 (the "Dark Web Monitoring Subclass").

California Subclass

All individuals residing in California whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach that occurred in, or around, April 2024 (the "California Subclass").

53. Collectively, the Class, Dark Web Monitoring Subclass, and California Subclass are referred to as the "Classes" or "Class Members."

54. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has 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.

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

56. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, 2.9 billion individuals were impacted in Data Breach.

57. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes 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 a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

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

d. Whether Defendant required its third-party vendors to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant had a duty to adequately, promptly, and accurately inform 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 practices, procedures, or 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 ongoing harm faced as a result of the Data Breach.

58. Typicality: Plaintiff's claims are typical of those of the other members of the Classes 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 Classes.

59. 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 Classes, 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 Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

60. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff 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 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.

61. 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.

62. 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 for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant 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 was exposed is representative of that experienced by the Classes 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.

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

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

65. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Classes, 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.

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

67. 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 Class Members of the Data Breach;

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

c. Whether Defendant's (or their vendors') security measures to protect its network were reasonable in light of industry best practices;

d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;

f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and

g. Whether adherence to FTC recommendations and best practices for protecting personal information would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT 1: NEGLIGENCE/NEGLIGENCE *PER SE* (*On behalf of Plaintiff and all Class Members*)

68. Plaintiff re-allege and incorporate by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

69. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members were unaware that Defendant was collecting and reselling their PII.

70. Defendant had full knowledge of the types of PII it collected and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

71. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII for commercial gain, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

72. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology and/or cloud environments; (ii) contractually obligated its vendors to implement reasonable administrative, technical, and physical measures to protect the PII from unauthorized disclosure; (iii) complied with applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits of Defendant's and/or its vendors' data processing activities; (v) regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) provided timely notice to

individuals impacted by a data breach event.

73. Defendant 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 or deceptive trade practices that affect commerce.

74. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII that Defendant was no longer required to retain.

75. Defendant had a duty to notify Plaintiff and Class Members of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any fraudulent usage of their PII.

76. Defendant violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII. Defendant's violations of Section 5 of the FTC Act, and other state consumer protection statutes, constitute negligence *per se.*

77. Defendant 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 Defendant includes, but are not limited to, the following:

a. Failing to implement organizational controls, including a patch management policy to track and manage updates and patches for known vulnerabilities.

b. Failing to have defined periods when patches must be installed and/or an automated means of determining what patches are needed, where they are needed, and the status of current patch levels by location.

c. Failing to encrypt personally identifying information in transit and at rest.

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

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

f. Allowing unauthorized access to PII.

g. Failing to detect in a timely manner that PII had been compromised.

h. Failing to remove former customers' PII it was no longer required to retain.

i. Failing to timely and adequately notify Plaintiff and 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.

j. Failing to implement data security practices consistent with industry best practices.

78. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

79. The injuries resulting to Plaintiff and Class Members because of Defendant's failure to use adequate security measures was reasonably foreseeable.

80. Plaintiff and Class Members were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of updating, patching, or fixing critical vulnerabilities in its network.

81. Plaintiff and Class Members had no ability to protect the PII in Defendant's possession. Defendant was in the best position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

82. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure to implement reasonable security measures to protect the PII of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

83. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

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

85. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 2: UNJUST ENRICHMENT
(*On behalf of Plaintiff and all Class Members*)

86. Plaintiff re-allege and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

87. By obtaining and reselling Plaintiff's and Class Members' PII, Defendant received a monetary benefit. Defendant knew that it could sell the PII for financial gain and has retained that benefit.

88. By collecting the PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

89. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that it received without paying Plaintiff and Class Members value in return.

90. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

91. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT 3: INVASION OF PRIVACY
(*On behalf of Plaintiff and all Class Members*)

92. Plaintiff re-allege and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

93. Plaintiff and Class Members had a legitimate expectation of privacy in their personally identifying information such as their social security numbers and dates of birth. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

94. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

95. Defendant permitted the public disclosure of Plaintiff's and Class Members' PII to unauthorized third parties.

96. The PII that was disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

97. Defendant permitted its information technology environment to remain vulnerable to foreseeable threats, which created an atmosphere for the Data Breach to occur. Despite knowledge of the substantial risk of harm created by these conditions, Defendant intentionally disregarded the risk, thus permitting the Data Breach to occur.

98. By permitting the unauthorized disclosure, Defendant acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PII at issue was not newsworthy or of any service to the public interest.

99. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and/or implement appropriate policies and procedures to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

100. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

101. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

/ / /

/ / /

COUNT 4: BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(*On behalf of Plaintiff and all Class Members*)

102. Plaintiff re-allege and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

103. Upon information and belief, Plaintiff and Class Members were the express, foreseeable, and intended beneficiaries of valid and enforceable contracts between Defendant and its customers that, upon information and belief, include obligations to keep sensitive PII private and secure.

104. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that they were made primarily and directly to benefit Plaintiff and Class Members and safeguard the PII entrusted to Defendant in the process of providing these services.

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

106. Defendant materially breached its contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized individuals during the Data Breach.

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

108. 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 but not limited to the release and disclosure of their PII, the loss of control of their PII, the risk of suffering additional damages, and out of pocket expenses.

109. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to (i) strength its data security systems and monitoring processes; (ii) submit to future annual audits of those systems and monitoring processes; and (iii)

immediately provide adequate credit and dark web monitoring services to all Class Members.

COUNT 5: BREACH OF IMPLIED CONTRACT
(*On behalf of Plaintiff and all Class Members*)

110. Plaintiff re-allege and incorporate by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

111. Defendant retained and maintained Plaintiff's and Class Members' PII in the course of doing business. Accordingly, Plaintiff and Class Members entered into implied contracts with Defendant when Defendant retained their PII, upon which Defendant agreed to safeguard and protect such information, keep it confidential, and timely notify Plaintiff and Class Members of any breach.

112. Plaintiff and Class Members fully perform their obligations under the implied contracts with defendant, which defendant initiated and voluntarily undertook. Plaintiff and class members conferred a monetary benefit to Defendant when they provided their PII and payment to Defendant's clients, who used defendants background check services.

113. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to secure and protect their PII and failing to notify Plaintiff and Class Members of the breach.

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

115. 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) lost benefit of the bargain; and the continued and certainly increased risk to their PII, which: (a) remains unencrypted

and available for unauthorized third parties to access an abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosure so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

COUNT 6: CALIFORNIA'S CONSTITUTIONAL RIGHT TO PRIVACY
(On behalf of Plaintiff and all California Subclass Members)

117. Plaintiff incorporates the foregoing allegations as though fully set forth herein.

118. Plaintiff and the California Subclass Members have reasonable expectations of privacy in PII. Plaintiff's and California Subclass Members' private affairs include their PII.

119. Defendant intentionally intruded on and into Plaintiff's and California Subclass Members' solitude, seclusion, right of privacy, or private affairs by intentionally collecting their PII with the knowledge that that PII would be stored unencrypted and susceptible to theft.

120. These intrusions are highly offensive to a reasonable person, because they disclosed sensitive and confidential information, constituting an egregious breach of social norms.

121. Plaintiff and the California Subclass Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

122. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and California Subclass Members.

123. As a result of Defendants' actions, Plaintiff and California Subclass Members seek damages and punitive damages in an amount to be determined at trial.

Plaintiff and California Subclass Members seek punitive damages because Defendants' actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiff and California Subclass Members and were made in conscious disregard of Plaintiff's and California Subclass Members' rights.

124. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT 7: CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT ("CLRA"), CAL. CIV. CODE § 1750, ET SEQ.
(*On behalf of Plaintiff and all California Subclass Members*)

125. Plaintiff incorporates the foregoing allegations as though fully set forth herein.

126. Defendant is a "person," under Cal. Civ. Code § 1761(c).

127. Plaintiff is a "consumer[]," as defined by Cal. Civ. Code § 1761(d), who purchased or leased a vehicle whose location data was collected by Defendants.

128. Defendants' conduct, as described herein, violates the CLRA. Specifically, Defendants violated the CLRA by omitting material facts and failing to disclose their data collection and transmission practices and engaging in the practices proscribed by Cal. Civ. Code § 1770(a) in transactions that were intended to result in, and did result in, the collection and dissemination of Plaintiff's and Class Members' location data.

129. Defendant violated the CLRA by selling services to consumers that while knowing that they collected PII that was likely to be transmitted to bad actors.

130. Defendant omitted from Plaintiff and other California Subclass Members the material fact that when their services were sold to Plaintiff, Plaintiff's PII was susceptible of being stolen and transmitted to bad actors. This is a fact that a reasonable consumer would consider important.

131. Defendant knew, at the time they sold Plaintiff and California Subclass Members their services, of the material fact that Plaintiff and the California Subclass Members' PII that was provided to Defendant as a condition of the transaction would be

stored unencrypted and was susceptible to theft and transmission to bad actors. Defendant's conduct was fraudulent, wanton, and malicious.

132. Defendant's unfair and deceptive acts or practices were the foreseeable and actual cause of Plaintiff and other California Subclass Members suffering actual damage.

133. Plaintiff and the other California Subclass Members paid for services that were supposed to meet certain specifications. When they received services that did not conform to these specifications, i.e., when they came at the cost of losing their PII to bad actors and facing a lifetime threat of identity theft, those services fell below the standards set by and described in Defendants' representations, upon information and belief, and Plaintiff and the other California Subclass Members were damaged on account of having their privacy invaded; their PII transmitted to third parties; and paying more than they would have for Defendant's goods and services had they known what they know now.

134. 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: invasion of privacy; theft of their PII; uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; loss of benefit of the bargain; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; statutory damages; nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in 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.

135. Pursuant to § 1782 of the CLRA, Plaintiff notified Defendant in writing by mail of the particular violations of § 1770 of the CLRA and demanded that Defendants rectify the problems associated with the actions detailed above and give notice to all

affected consumers of Defendant's intent to so act. Plaintiff sent his notice letter on September 18, 2024.

136. If Defendant fails to rectify or agree to rectify the problems associated with the actions detailed above and give notice to all affected consumers within 30 days of the date of written notice pursuant § 1782 of the Act, Plaintiff will amend this Complaint to add claims for actual, punitive, and statutory damages, as appropriate.

137. Pursuant to § 1780(d) of the Act, attached hereto as Exhibit A is the affidavit showing that this action has been commenced in the proper forum.

COUNT 8: CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL"), CALIFORNIA BUSINESS & PROFESSIONS CODE § 17200, ET SEQ.
(O*n behalf of Plaintiff and all California Subclass Members)*

138. Plaintiff incorporates the foregoing allegations as though fully set forth herein.

139. The UCL prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising. In the course of conducting business, Defendants committed "unlawful" business practices by, among other things, upon information and belief, making the representations and omissions of material facts, as set forth more fully herein, and violating Civil Code §§ 1572, 1573, 1709, 1711, 1770(a)(5), (6), (7), (9), and (16), and Business & Professions Code §§ 17200, et seq., 17500, et seq., and the common law.

140. In the course of conducting business, Defendants committed "unfair" business practices by, among other things, collecting Plaintiffs' and Class Members' PII without their knowledge and failing to prevent its disclosure to unauthorized third parties.

141. Plaintiff and the California Subclass Members relied on Defendant's false representations and promises when entering contracts with Defendant to acquire goods and services and accepting Defendant's terms.

142. 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.

143. Upon information and belief, Defendant misrepresented and omitted material facts regarding the characteristics, capabilities, and benefits of services they provided, including the fact that Plaintiff and the California Subclass Members' PII was stored unencrypted and susceptible to theft and use by bad actors. There is no societal benefit from such false and misleading representations and omissions, only harm.

144. While Plaintiff and other California Subclass Members were harmed by this conduct, Defendants were unjustly enriched. As a result, Defendants' conduct is "unfair" as it has offended an established public policy. Further, Defendants engaged in immoral, unethical, oppressive, and unscrupulous activities that are substantially injurious to consumers.

145. Defendant knew or should have known at the time that it sold its services t that that the PII that they collected and maintained would be targeted by cybercriminals.

146. Plaintiff alleges violations of consumer protection, unfair competition, and truth in advertising laws in California, resulting in harm to consumers. Defendants' acts and omissions also violate and offend the public policy against engaging in false and misleading advertising, unfair competition, and deceptive conduct towards consumers. This conduct constitutes violations of the UCL's "unfair" prong. There were reasonably available alternatives to further Defendants' legitimate business interests other than the conduct described herein.

147. The UCL also prohibits any "fraudulent business act or practice." In the course of conducting business, Defendants committed "fraudulent business act[s] or practices" by, among other things, making the representations and omissions of material facts regarding the safety and security of Plaintiff's and California Subclass Members' PII.

148. Defendants' actions, claims, omissions, and misleading statements, as more fully set forth above, were also false, misleading, and likely to deceive the

consuming public within the meaning of the UCL.

149. Plaintiff and California Class Members were deceived as a result of their reliance on Defendants' material representations and omissions, which are described above. Plaintiff and other California Subclass members suffered injury in fact and lost money as a result of purchasing deceptively advertised goods and services by having their privacy invaded; their PII collected and transmitted to third parties; paying more than they would have for Defendant's goods and services had they know what they now; and incurring other consequential inconvenience, aggravation, damages, and loss of money and time.

150. Unless restrained and enjoined, Defendants will continue to engage in the above-described conduct. Accordingly, injunctive relief is appropriate.

151. Plaintiff, on behalf of himself and all others similarly situated, seeks restitution from Defendants of all money obtained from Plaintiff and the other members of the California Subclass collected as a result of unfair competition, an injunction prohibiting Defendants from continuing such practices, corrective advertising, and all other relief this Court deems appropriate, consistent with Business & Professions Code § 17203.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as the representatives for the Classes and counsel for Plaintiff as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statues and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and Class Members on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring and dark web scanning services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and Class Members their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

Dated: September 18, 2024 **BRADLEY/GROMBACHER LLP**

By: /s/ Kiley L. Grombacher
Kiley L. Grombacher
Attorneys for Plaintiff and others similarly situated

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: September 18, 2024 **BRADLEY/GROMBACHER LLP**

By: /s/ Kiley L. Grombacher
Kiley L. Grombacher
Attorneys for Plaintiff and others similarly situated