John C. Bohren (CA Bar No. 295292)
YANNI LAW APC
yanni@bohrenlaw.com
145 South Spring Street, Suite 850
Los Angeles, CA 90012
Telephone: (619) 433-2803

Paul J. Doolittle (pro hac forthcoming)
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff and Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

RICKY SULLIVAN, individually and on behalf of all others similarly situated, **Plaintiff(s),** **vs.** **PROSPER FUNDING, LLC, and PROSPER MARKETPLACE, INC.,** **Defendant(s).**	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Ricky Sullivan ("Plaintiff") brings this Class Action Complaint against Defendants, Prosper Funding, LLC, and Prosper Marketplace, Inc., ("Defendants") individually, 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:

JURISDICTION & VENUE

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

2. This Court has personal jurisdiction over Defendants because their principal place of business is in this District. Defendants have also purposefully availed themselves of the laws, rights, and benefits of the State of California.

3. Venue is proper under 28 U.S.C §1391(b) because Defendants maintain a principal place of business in this District and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

PARTIES

4. Plaintiff Ricky Sullivan is a resident and citizen of Carbondale, Illinois.

5. Defendant, Prosper Funding LLC, maintains a principal place of business at 221 Main Street, 3rd Floor, San Francisco, San Francisco County, California 94105. Defendant may be served via its registered agent, CSC - Lawyers Incorporating Service, 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California 95833.

6. Defendant, Prosper Marketplace Inc., maintains a principal place of business at 221 Main Street, 3rd Floor, San Francisco, San Francisco County, California 94105. Defendant may be served via its registered agent, CSC - Lawyers Incorporating Service, 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California 95833.

7. Defendant Prosper Funding LLC owns a peer-to-peer online marketplace where customers can apply for unsecured personal loans. Defendant Prosper Funding LLC is a subsidiary of Defendant Prosper Marketplace Inc.

FACTUAL ALLEGATIONS

8. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard the personally identifiable information ("PII") of its customers, including, but not limited to Social Security numbers.

9. Defendants are institutions that are significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, such as servicing loans, financial planning, and credit monitoring. Defendants require customers to provide their PII in connection with the transaction.

10. Plaintiff is a customer of Defendants' various financial services. During their relationship, Plaintiff provided Defendants with at least the following: full name, date of birth, contact information, and Social Security number.

11. Defendants promised to use reasonable technical, administrative, and physical safeguards to protect the PII it collected. These promises were contained in the applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

12. For instance, Defendants' published privacy policy provides, "Prosper uses significant safeguards, including physical, technical (electronic), and operational controls to protect your personal information, both during transmission and once received… Once on our system, personal information can only be read or written through defined service access points, the use of which is password-protected. Data security is achieved through technical safeguards that include a combination of encryption, firewalls, intrusion prevention system, malware detection system, and data loss prevention systems. Prosper also conducts vulnerability scans of applications and systems regularly. Access to the system is tightly controlled and limited to only those who have a need to access information. Administrative safeguards such as a security awareness program, background

checks, and internal information use policy ensure that only trained and trusted staff are permitted to access personal information."[1]

13. Plaintiff, as a customer of Defendants, relied on these representations and on these sophisticated business entities to keep his PII confidential, securely maintained, and to make only authorized disclosures of this information.

14. On, or about, September 1, 2025, Defendants discovered that an unauthorized party gained access to its network and determined that Plaintiff's personal information—which was entrusted to Defendants on the mutual understanding that Defendants would protect it against unauthorized disclosure—was accessed and exfiltrated in a data breach (hereafter referred to as the "Data Breach").

15. Defendants' investigation into the Data Breach revealed that confidential, proprietary, and personal information, including Social Security numbers, was obtained through unauthorized queries made on databases that store customer and applicant data.[2]

16. On, or about, September 17, 2025, Defendants sent out data breach notice letters to individuals who were affected by the data breach. Omitted from the data breach notice letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff, who retains a vested interest in ensuring that their PII remains protected.

17. Plaintiff received an e-mail notice of the Data Breach from Defendants on September 17, 2025.

[1] *See,* Prosper Privacy Policy, available here: https://www.prosper.com/legal/privacy-policy

[2] https://www.sec.gov/Archives/edgar/data/1542574/000141626525000038/prosper-20250901.htm

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

19. The Data Breach was a direct result of Defendant's failure to implement an information security program designed to: (a) to ensure the security and confidentiality of customer information; (b) to protect against anticipated threats or hazards to the security or integrity of that information; and (c) to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.

20. An information security program encompasses the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. Had Defendants implemented an information security program consistent with industry standards and best practices, it could have prevented the Data Breach.

21. As a result of the Data Breach, Plaintiff has suffered an actual injury, similar to an intangible harm remedied at common law. Defendants' failure to implement an information security program 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. The injuries Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

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

23. Defendants' 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.

24. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [3] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[4]

25. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [5] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[6]

26. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and 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 illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

---

[3] *See*,https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.

[4] *Id.*

[5] *See*,https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.

[6] *Id.*

[7] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

27. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[8] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[9]

28. Note, it is not an 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.

29. 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."[10]

30. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security numbers are: arguably "the most dangerous

[8] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/
[9] *See* https://www.investopedia.com/terms/s/ssn.asp
[10] 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

type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

31. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[11]

32. 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 the Plaintiff.

33. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused him to: (i) implement a security freeze to help prevent new accounts from being opened in his name; (ii) lose time and effort spent responding to the Data Breach; and/or (iii) experience emotional distress associated with reviewing accounts for 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.

34. 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,

[11] *See* https://oag.ca.gov/idtheft/facts/your-ssn

taking out loans, using Plaintiff's information to obtain government benefits, file fraudulent tax returns, obtain driver's licenses, and give false information to police during an arrest.

35. As a result of the Data Breach, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) statutory damages; (vi) nominal damages; and (vii) 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.

36. 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.

The Data Breach Was Avoidable

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

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

39. Upon information and belief, the Data Breach occurred because Defendants' information repositories were improperly secured, which permitted an unauthorized party to access Plaintiff's sensitive personal data.

40. To detect and prevent the Data Breach, Defendants could and should have implemented the following measures:

Reasonable Safeguards

a. 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.

b. Periodically review accounts and privileges for critical and sensitive information repositories. Ensure that repositories such as cloud-hosted databases are not unintentionally exposed to the public and permit only necessary and authorized hosts to access them.

c. Implement multifactor authentication.

d. Implement data retention policies to automate periodically archiving and/or deleting data that is no longer needed.

e. 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.

f. 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.

g. Develop and publish policies that define acceptable information to be stored in repositories.

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

i. 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.

j. 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.

k. 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.

l. 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.

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

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

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

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

q. 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.

r. 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.

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

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

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

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

w. Conduct an annual penetration test and vulnerability assessment.

x. Secure your backups.[12]

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

z. 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.

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

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

cc. 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.

---

[12] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

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

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

ff. 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.

gg. 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.

hh. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[13]

41. The Federal Trade Commission's Standards for Safeguarding Customer Information (the "Safeguards Rule") 16 CFR §314, requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The primary requirements of an information security program are:

a. Designate a qualified individual to implement and supervise the information security program.

b. Conduct an assessment to determine foreseeable risks and threats – internal and external – to the security, confidentiality, and integrity of customer information.

c. Design and implement safeguards to control the risks identified through the risk assessment.

d. Regularly monitor and test the effectiveness of the chosen safeguards.

e. Provide staff with security awareness training and schedule regular refreshers.

f. Select service providers with the skills and experience to maintain appropriate safeguards. Include security expectations in vendor contracts, monitor the service provider's work, and provide for periodic reassessments of their suitability.

g. Ensure the information security program remains current. It should reflect changes to operations, changes based on information gained from risk assessments, changes due to emerging threats, changes in personnel, and changes necessitated by other circumstances that may have a material impact on the information security program.

[13] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

h. Create a written incident response plan.

i. Require the "Qualified Individual" to report to the Board of Directors, in writing, at least annually.[14]

42. Given that Defendants are financial institutions that collected, used, and stored PII, Defendants could and should have identified the risks and potential effects of collecting, maintaining, and sharing personal information.

43. Without identifying the potential risks to the personal data in Defendants' possession, Defendants could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures, resulting in the Data Breach and the exposure of Plaintiff and the Class Members' PII.

44. Defendants knew and understood unencrypted PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant times, Defendants 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 the Class Members as a result.

Plaintiff and Class Members Sustained Damages in the Data Breach

45. Plaintiff Ricky Sullivan received an email notice from Defendants on September 17, 2025, regarding the Data Breach. Plaintiff Sullivan would not have allowed Defendants to maintain his sensitive information if he knew Defendants would not implement reasonable safeguards to protect the data from unauthorized access and disclosure.

46. Plaintiff Sullivan is very careful about maintaining the privacy and security of his PII. Plaintiff Sullivan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. The Data Breach has caused Plaintiff to suffer

[14] See, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

fear, anxiety, and stress. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring financial accounts, and placing security freezes with the credit bureaus. Plaintiff anticipates spending additional time and/or money to investigate and mitigate the consequences of the Data Breach.

47. The invasion of the Plaintiff 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.

48. 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 Defendants' conduct.

49. 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 likely acquired in the Data Breach and potentially released on the dark web. The substantial risk of future exploitation created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

50. 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.[15] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

51. Given the type of targeted attack in this case, the sophistication of the criminal responsible for the Data Breach, the type of PII involved in the Data Breach, hacker behaviors 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, or will be placed, on the dark web, it is reasonable for Plaintiff and the 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.

52. 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 time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

53. 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

[15] "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

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.[16]

54. 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.

55. As a result of the Data Breach, Plaintiff 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.

56. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[17] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[18] Sensitive PII can sell for as much as $363 per record.[19]

57. Furthermore, Defendants' poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members, collecting their 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.

---

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

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

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

[19] *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).

58. When agreeing to pay Defendants for products or services, consumers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendants did not invest the funds into implementing reasonable data security practices. 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 Defendants.

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

CLASS ALLEGATIONS

60. 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.

61. The Class that Plaintiff seeks to represent is 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 a data breach that occurred on, or about, September 1, 2025, as reported by Defendants (the "Class" or "Class Members").

62. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' 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.

63. 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.

64. Numerosity: 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.

65. 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 Defendants had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

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

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

e. When Defendants actually learned of the Data Breach;

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

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

h. Whether Defendants adequately addressed and fixed the practices, procedures, or vulnerabilities which permitted the Data Breach to occur;

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

j. 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.

66. 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.

67. 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 Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff challenges 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.

68. 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.

69. 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 Defendants. 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.

70. 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 Defendants would necessarily gain an unconscionable advantage since Defendants 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 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.

71. The litigation of the claims brought herein is manageable. Defendants' 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.

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

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

74. Further, Defendants have 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.

75. Likewise, the following issues 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 issues include, but are not limited to:

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

b. Whether Defendants' (or their vendors') security measures were reasonable in light of industry best practices;

c. Whether Defendants' (or their vendors') failure to institute adequate data protection measures amounted to negligence;

d. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII;

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

f. 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/WANTONNESS

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

77. Defendants require their customers to submit PII in the ordinary course of providing products or services.

78. Defendants gathered and stored the PII of Plaintiff and Class Members as part of its business. Plaintiff and Class Members entrusted Defendants with their PII with the understanding that Defendants would adequately safeguard their information.

79. Defendants 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.

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

81. Defendants are financial institutions and have a duty to develop, implement, and maintain a written information security program designed to protect customer information. The information security program must be appropriate to the size and complexity of the business, the nature and scope of business activities, and the sensitivity of the information at issue.

82. Defendants' information security program must be designed to: (a) ensure the security and confidentiality of customer information; (b) protect against anticipated threats or hazards to the security or integrity of that information; and (c) protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.

83. Defendants' 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 adhere to the requirements of Defendant's privacy policy; (iii) complied with the Safeguards Rule and other 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.

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

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

86. Defendants violated its common law duty, the Safeguards Rule, and other state consumer protection statutes by failing to implement an information security plan or use reasonable security measures to protect PII. Defendant's violations constitute negligence and/or wantonness.

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

a. Failing to designate a qualified individual to implement and supervise its information security program.

b. Failing to conduct an assessment to determine foreseeable risks and threats – internal and external – to the confidentiality and integrity of customer information.

c. Failing to design and implement safeguards to control the risks identified through the risk assessment.

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

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

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

g. Allowing unauthorized access to PII.

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

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

j. Failing to implement data security practices consistent with Defendant's published privacy policies.

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

89. Plaintiff was 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.

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

91. But for Defendants' breach of duties owed to Plaintiff and the Class, their PII would not have been compromised. There is a close causal connection between Defendants' failure to implement reasonable 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.

92. 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) statutory damages; (vii) nominal damages; and (viii) 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.

93. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

94. 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: BREACH OF IMPLIED CONTRACT

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

96. Defendants require their customers to submit PII in the ordinary course of providing financial products or services.

97. Defendants published a privacy policy to inform the public about how Defendants collect, use, share, and protect the information Defendants gather in connection with the provision of those products or services.

98. In so doing, Plaintiff and Class Members entered implied contracts with Defendants by which Defendants agreed to use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information it collects and stores.

99. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of an expressed or implied promise to implement reasonable data protection measures.

100. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant.

101. Defendants breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on the Defendants' web site, privacy policy, and in other documents, all of which created a reasonable expectation that the personal information Defendants collected would be adequately protected and that the Defendants would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

102. As a direct and proximate result of the Defendants' breach of an implied contract, 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) statutory damages; (vii) nominal damages; and (viii) 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.

103. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants 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 3: UNJUST ENRICHMENT

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

105. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

106. By providing their PII, Plaintiff and Class Members conferred a monetary benefit on Defendants. Defendants used the PII to market, advertise, and sell additional services to Plaintiff and Class Members. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit.

107. By collecting the PII, Defendants were 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.

108. Defendants failed to secure Plaintiff and Class Members' PII and, therefore, it would be unjust for Defendants to retain any of the benefits that Plaintiff and Class Members conferred upon Defendants without paying value in return.

109. As a direct and proximate result of the Defendants' 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) statutory damages; (vii) nominal damages; and (viii) 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 Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

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

COUNT 4: INVASION OF PRIVACY

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

112. Plaintiff and Class Members had a legitimate expectation of privacy in their personally identifying information such as their Social Security numbers, dates of birth, and credit scores. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

113. Defendants owed a duty to Plaintiff and Class Members to keep their PII confidential.

114. Defendants permitted the public disclosure of Plaintiff and Class Members' PII to unauthorized third parties.

115. The PII that was disclosed without the proper 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.

116. Defendants 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.

117. By permitting the unauthorized disclosure, Defendants acted with reckless disregard for the Plaintiff 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.

118. Defendants 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.

119. Defendants acted with such reckless disregard as to the safety of Plaintiff 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.

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

COUNT 5: VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT (815 ILCS 505/2)

121. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

122. Plaintiff and Class Members are consumers of Defendants' financial products and services. Defendants require its customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing products or services.

123. Defendants gathered and stored the PII of Plaintiff and Class Members as part of its business. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendants would adequately safeguard their information.

124. Defendants misrepresented, concealed, suppressed, or omitted material facts regarding its data safeguards, including physical, technical, and operational controls to protect personal information, which were facts material to Plaintiff and Class Members, with the intent that Plaintiff and Class Members rely on said representations or omissions when using Defendants' platform. Such behavior by Defendant constitutes a deceptive act under Illinois law.

125. Under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies.

126. Defendants violated the Illinois consumer protection statute by failing to adhere to its own privacy policy regarding the security of Plaintiff and Class Members' information.

Defendants further violated the state consumer protection statute by failing to use reasonable measures to protect PII.

127. Defendants' conduct created a likelihood of confusion or misunderstanding regarding its actual data privacy and security practices. Defendants promised to protect Plaintiff and Class Members' PII via its privacy policies, but allowed the unauthorized access to this sensitive personal information; Defendants failed to disclose material facts that the Plaintiff and Class Members' PII would be disclosed to unauthorized third parties; Defendants failed to obtain Plaintiff and Class Members' consent in transmitting their PII to a third party; and knowingly violated industry and legal standards regarding the protection of Plaintiff and Class Members' PII.

128. Defendants' unfair or deceptive acts affected public interests, including those of Plaintiff and Class Members. Defendants knew or should have known that it was likely to mislead its customers who were acting reasonably. Defendants engaged in unfair or deceptive practices by breaching its duties to provide technical and organizational data security policies, procedures, and practices. Defendants' failure to adhere to its published privacy policies and procedures is offensive to established public policy and is substantially injurious to consumers as evidenced by the massive Data Breach.

129. Had Plaintiff and Class Members known Defendants would not follow its own published security practices they would not have purchased (or continued to purchase) Defendants' products or services. Defendants' deceptive acts, as described herein, proximately caused Plaintiff and Class Members damages.

130. As a direct and proximate result of the Defendants' conduct, Plaintiff and Class Members suffered damages 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) mitigation costs and expenses; and (vii) attorneys' fees and court costs.

131. Plaintiff alleges that Defendants' data security measures remain inadequate. Plaintiff will 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 the future.

132. Plaintiff and Class Members have suffered irreparable injury, and will continue to suffer injury in the future, as a result of Defendants' deceptive trade practices, which places Plaintiff and Class Members at imminent risk that further compromises of their PII will occur in the future. As such, the remedies available at law are inadequate to compensate for that injury. Accordingly, Plaintiff and Class Members also seek to obtain a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes.

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class Members' PII.

133. The Court also should issue corresponding prospective injunctive relief requiring that Defendants employ adequate data protection practices consistent with law and industry standards.

134. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

135. The issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendants to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the multitude of individuals whose PII would be at risk of future unauthorized disclosures.

136. As a result of the Defendants' false, misleading, or deceptive acts, regarding its data security practices, the consuming public in general, Plaintiff and Class Members suffered injuries including, but not limited to, the future and continued risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains under Defendants' 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.

137. Plaintiff and Class Members are entitled to attorneys' fees, costs, and injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing information repositories; and (iii) to provide adequate dark web monitoring, identity theft protection, and/or credit monitoring to all affected by the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class 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(s) as the representatives for the Class and counsel for Plaintiff(s) as Class Counsel;

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

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

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

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 the Class 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.

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 25, 2025.

Respectfully Submitted,

/s/ John C. Bohren
John C. Bohren (Bar No. 295292)
YANNI LAW APC
145 South Spring Street, Suite 850
Los Angeles, CA 90012
Telephone: (619) 433-2803
yanni@bohrenlaw.com

-AND-

Paul J. Doolittle (pro hac forthcoming)
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff and Proposed Class