BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
pbrown@bholaw.com

NUSSBAUM LAW GROUP, P.C.
LINDA P. NUSSBAUM (*pro hac vice forthcoming*)
TANYA KORKHOV (*pro hac vice forthcoming*)
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Tel: 917/438-9189
lnussbaum@nussbaumpc.com
tkorkhov@nussbaumpc.com

[Additional Counsel appear on signature page]

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ADA RIVERA, individually, and on behalf of all others similarly situated, Plaintiff, v. PROSPER FUNDING LLC and PROSPER MARKETPLACE, INC., Defendants.	Case No. 3:25-cv-09133 **CLASS ACTION COMPLAINT** **CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Ada Rivera ("Plaintiff"), by and through her undersigned counsel, on behalf of herself and a class of all other similarly situated persons, files this Class Action Complaint against Prosper Funding LLC ("Prosper Funding") and Prosper Marketplace, Inc. ("Prosper Marketplace") and, together with Prosper Funding, ("Prosper" or "Defendants"). Plaintiff's allegations are made based upon personal knowledge, her own acts, and upon information and belief and investigation of counsel, as to all other matters.

NATURE OF THE ACTION

1. Plaintiff brings this action against Defendants for their failure to properly secure and safeguard highly valuable, protected, personally identifiable information and for their failure to comply with industry standards to protect information systems that contain and/or are utilized to transfer PII (defined *infra*). Plaintiff has been, and continues to be, harmed as a result of Defendants' failure to properly secure and safeguard their customers' highly valuable, protected, personally identifiable information including, *inter alia*, their customers' names, dates of birth, Social Security numbers, and more (collectively, "PII" or "Personal Information" or "Private Information"); and for their failure to comply with industry standards to protect information systems that contain PII.

2. Defendant Prosper Funding is a limited liability company that services loans, manages borrower and investor relationships, and offers tools for financial planning and credit monitoring.[1]

3. Defendant Prosper Funding is a subsidiary of Defendant Prosper Marketplace, a financial services company that operates a number of websites including www.prosper.com, www.prospercards.com, www.myprospercard.com, and www.prosperhealthcare.com.[2]

4. As financial services companies, Defendants store a litany of highly sensitive PII collected from their current and former customers.

5. Defendants lost control over that data when cybercriminals infiltrated their insufficiently protected computer systems in a data breach (the "Data Breach").

[1] *See* Prosper Privacy Policy & Federal Privacy Notice, Information Prosper Collects About You, PROSPER, https://www.prosper.com/legal/privacy-policy (last visited Oct. 22, 2025).

[2] *See id.*

6. Upon information and belief, on or about September 2, 2025, cyber criminals performed unauthorized queries on Defendants' customer databases. This gave them access to a host of sensitive records, including: full names and home addresses, dates of birth, Social Security numbers, government-issued identification numbers, e-mail addresses and employment details, credit status and income levels, and IP addresses and browser user-agent strings.[3]

7. As a direct and proximate result of Defendants' negligent failure to implement reasonable data security measures, Plaintiff's and Class members' PII are now in the hands of cyber criminals.

8. Plaintiff and Class members are now at a significantly increased and certainly impending risk of fraud, extortion, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks which may last for the rest of their lives. Consequently, Plaintiff and Class members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiff brings claims including negligence, negligence *per se*, unjust enrichment, and breach of implied contract, seeking damages and injunctive relief, including the adoption of reasonably sufficient data security practices to safeguard the PII in Defendants' possession, in order to prevent incidents like the Data Breach from recurring in the future.

PARTIES

10. Plaintiff, at all relevant times, was a citizen of the State of California and a resident of San Bernardino County.

11. Defendant Prosper Funding LLC is a Delaware limited liability company, maintaining its principal place of business at 221 Main Street, 3rd Floor, San Francisco, California, 94105.

12. Defendant Prosper Marketplace, Inc. is a Delaware corporation maintaining its principal place of business at 221 Main Street, 3rd Floor, San Francisco, California, 94105.

[3] Security Daily Review, Prosper Data Breach: 17.6 Million Accounts Compromised (Oct. 22, 2025), https://dailysecurityreview.com/cyber-security/data-security/prosper-data-breach-17-6-million-accounts-compromised/ (last visited Oct. 22, 2025).

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because Plaintiff and at least one member of the Class, as defined below, are citizens of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

14. This Court has general personal jurisdiction over Defendants because Defendants' principal places of business are located in this District, Defendants regularly conduct business in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

15. Venue is proper under 28 U.S.C. § 1391(a)(2), (b)(1)-(3), and (c)(2) because Defendants' principal places of business are located in this District, Defendants conduct substantial business in this District, and a substantial part of the events giving rise to the claims emanated from activities within this District.

FACTUAL ALLEGATIONS

A. Defendants' Business

16. Defendant Prosper Funding is a limited liability company that services loans, manages borrower and investor relationships, and offers tools for financial planning and credit monitoring.

17. Prosper Funding is a subsidiary of Defendant Prosper Marketplace.

18. Prosper Marketplace operates an online peer-to-peer (P2P) lending platform that seeks to "democratize access to credit and advance financial well-being" by connecting individual and institutional investors with creditworthy borrowers.[4]

19. In the ordinary course of business, Defendants collect a wealth of Personal Information from their customers, including:

- **Identity Verification Information** – including your name, address, email, telephone number, date of birth, Social Security number, driver's license number, passport number,

[4] About, Prosper (2025), https://www.prosper.com/about (last visited Oct. 22, 2025).

government-issued identification details, and similar information to verify your identity. …

- **Employment Information –** including your employment and income information.
- **Financial Information –** such as your bank account information or mortgage account number(s).
- **Account or Application Information –** such as your account number (including credit card number and details), account history, account balances, loan details, credit and income information, enrollment in offers or alerts, demographic information (where permitted or required by applicable law), the location and value of the property secur[ing] your loan, payment history, complaint information, and transaction and purchasing data. For a loan to be used with a merchant or service provider (e.g., a healthcare provider), the identity of the merchant or service provider and the name of the party that will receive the good or service.
- **Audio and Visual Information –** including audio, electronic, or similar information we capture through your communications with us, e.g., voice recordings of telephone conversations, emails and instant messaging.

***

- **Investor information –** If you register as an investor through Prosper, we collect information about your transactions and activity, including your fund transfers and purchases.
- **Other Personal Information You Provide Us –** including third-party bank information to complete a funds transfer, information you enter into a survey or chat, or any other information you may provide when using Prosper Websites or services.
- **Co-Applicant Personal Information –** We may also collect information that you provide to us about your co-applicant in connection with a joint application or loan. By submitting information about someone other than yourself, you represent that you are authorized to provide us with that person's information for the purposes identified in this Privacy Policy and/or in connection with our services.[5]

20. If a customer checks his or her rate or applies for credit through Defendants, Defendants collect additional information from credit bureaus and other third parties, including: credit scores, credit history, bank account information and bank transactions.[6]

[5] *See* Prosper Privacy Policy & Federal Privacy Notice, Information Prosper Collects About You, PROSPER, https://www.prosper.com/legal/privacy-policy (last visited Oct. 22, 2025).

[6] *Id.*

21. Defendants made promises and representations to Plaintiff and Class members, that the PII they solicited and collected from them would be kept safe and confidential, that the privacy of their information would be maintained, and that Defendants "use[] significant safeguards, including physical, technical (electronic), and operational controls to protect your personal information, both during transmission and once received."[7]

22. Plaintiff and Class members had the reasonable expectation that Defendants would comply with their obligations related to their customers' PII. Defendants owed Plaintiff and Class members a duty to provide reasonable security, consistent with industry standards and requirements, and to ensure that the Defendants' computer systems, networks, and protocols adequately protected their PII.

23. Defendants failed to comply with their obligations, resulting in the Data Breach.

B. The Data Breach

24. Despite Defendants' promise that access to their data system is "tightly controlled and limited to only those who have a need to access information,"[8] on or around September 2, 2025, Defendants discovered that an unauthorized party had gained access to their network and that a wide swath of PII from over 17.6 million customers and loan applicants—which was entrusted to Defendants on the mutual understanding that Defendants would protect it against unauthorized disclosure—had been accessed and exfiltrated.[9]

25. Although Defendants have not disclosed detailed root cause indicators, TechRepublic, an online trade publication for IT professionals, reported that attackers gained access through compromised credentials, suggesting weak or improperly secured account access possibly at the admin or database level.[10]

---

[7] *Id.*

[8] *Id.*

[9] Security Daily Review, Prosper Data Breach: 17.6 Million Accounts Compromised (Oct. 22, 2025), https://dailysecurityreview.com/cyber-security/data-security/prosper-data-breach-17-6-million-accounts-compromised/ (last visited Oct. 22, 2025).

[10] *Id.*

26. On September 17, 2025, Defendants emailed notice to Plaintiff and Class members informing them of the Data Breach (the "Notice") and confirming "that certain personal information, including Social Security Numbers, was obtained."[11]

27. According to industry reporting on the Data Breach, "[t]he breach also included metadata—such as user-agent and connection information—that could be used to fingerprint devices and assist in future social engineering or fraud attempts … [including] highly targeted phishing attacks, financial fraud, and potential synthetic identity creation."[12]

28. In the Notice, Defendants did not provide any assurances that all personal data has been either recovered or destroyed or that Defendants have sufficiently improved their data security practices to the extent necessary to avoid a future similar intrusion into their systems.[13]

29. Plaintiff and Class members now face years of constant surveillance of their financial and personal records.

C. The Data Breach was a Foreseeable Risk of which Defendants Were on Notice

30. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiff's and Class members' PII, including basic encryption techniques freely available to Defendants.

31. As sophisticated business entities handling confidential customer data, Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries, such as the financial services industry, that collect and store significant amounts of PII.

32. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding their current and former customers' PII, including Social Security

[11] *See* Notice of Cybersecurity Incident (attached hereto as **Exhibit A**).

[12] Security Daily Review, Prosper Data Breach: 17.6 Million Accounts Compromised (Oct. 22, 2025), https://dailysecurityreview.com/cyber-security/data-security/prosper-data-breach-17-6-million-accounts-compromised/ (last visited Oct. 22, 2025).

[13] *See* Notice of Cybersecurity Incident.

numbers and dates of birth, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Defendants' customers as a result of a breach.

33. In light of recent high profile data breaches at other financial services entities, Defendants knew or should have known that their electronic records and their customers' PII would be targeted by cybercriminals.

34. Cyberattacks and data breaches of financial services companies are especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[14]

D. The Value of Private Information and Effects of Unauthorized Disclosure

35. Defendants were well aware that the protected PII which they acquire is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

36. Defendants also knew that a breach of their computer systems, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

37. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

[14] UpGuard, 10 Biggest Data Breaches in Finance (July 10, 2025), https://www.upguard.com/blog/biggest-data-breaches-financial-services (last visited Oct. 22, 2025).

[15] 17 C.F.R. § 248.201(b)(9) (2013).

[16] *Id.* at § 248.201(b)(8)(i).

38. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web to obtain it.

39. Numerous sources cite dark web pricing for stolen identity credentials.[17] For example, Private Information can be sold at a price ranging from $40 to $200.[18] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[19]

40. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

41. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; and/or file a fraudulent tax return using the victim's information.

42. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

43. Moreover, the fraudulent activity resulting from a data breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:[20]

---

[17] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 22, 2025).

[18] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 22, 2025); *see also* Ben Luthi, *Here's What Your Data Sells for on the Dark Web*, Experian (June 30, 2025), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 22, 2025).

[19] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 22, 2025).

[20] PERSONAL INFORMATION Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 22, 2025).

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

44. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[21] Such fraud may go undetected until debt collection calls commence months, or even years later.

45. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[22]

46. Each of these fraudulent activities is difficult to detect. An individual may not know that his or his Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

47. Moreover, it is not an easy task to change or cancel a stolen Social Security number:[23]

> Getting a new Social Security number requires a lot of paperwork, including evidence of problems caused by misuse. Even then … a new number is not always helpful. The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.

48. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market."[24]

---

[21] *Identity Theft and Your Social Security Number*, Social Security Administration (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 22, 2025).

[22] *Id*.

[23] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Oct. 22, 2025).

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 22, 2025).

49. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—Social Security numbers, addresses, and dates of birth—is impossible to "close" and difficult, if not impossible, to change.

E. Defendants Failed to Comply with FTC Guidelines and Industry Best Practices

50. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be a factor in all business decision-making.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[26]

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

[25] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Oct. 22, 2025).

[26] *Id.*

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

54. Defendants failed to properly implement basic data security practices.

55. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

56. Defendants were (or should have been) at all times fully aware of their obligation to protect the PII they had collected from their customers and potential customers. Defendants were also aware (or should have been) of the significant repercussions that would result from their failure to do so.

F. Defendants Failed to Comply with Industry Standards

57. As shown above, experts studying cybersecurity routinely identify financial services providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

58. Several best practices have been identified that at a minimum should be implemented by financial service providers like Defendants, including but not limited to: employee education; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, i.e., making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

59. Other best cybersecurity practices that are standard in the financial industry include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

G. Plaintiff and Class Members Suffered Damages

60. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Defendants have done nothing to compensate Plaintiff or Class members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class members as a result of the Data Breach.

61. Plaintiff and Class members have been damaged by the compromise of their Private Information in the Data Breach.

62. Since learning of the Data Breach, Plaintiff and Class members have spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

63. Due to the Data Breach, Plaintiff and Class members anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

64. Plaintiff's and Class members' Private Information was compromised as a direct and proximate result of the Data Breach.

65. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

66. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have been forced to spend time dealing with the effects of the Data Breach.

67. Plaintiff and Class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

68. Plaintiff and Class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class members' Private

Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class members.

69. Plaintiff and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

70. Plaintiff and Class members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in similar cases.

71. Plaintiff and Class members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class members paid to Defendants was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiff's and Class members' Private Information. Thus, Plaintiff and Class members did not get what they paid for and agreed to.

72. Plaintiff and Class members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

73. Plaintiff and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and searching for, *inter alia*, fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

74. Moreover, Plaintiff and Class members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

75. Further, as a result of Defendants' conduct, Plaintiff and Class members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment, extortion, and depriving them of any right to privacy whatsoever.

76. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

H. Plaintiff's Experience

77. Plaintiff gave Defendants her PII as a condition to receiving Defendants' services.

78. In order to utilize Defendants' services, Plaintiff was required to entrust Defendants with her PII. In collecting and maintaining Plaintiff's PII, Defendants undertook a duty to act reasonably in their handling of Plaintiff's PII. Defendants, however, did not take reasonable care of Plaintiff's PII, leading to its exposure and compromise as a direct result of Defendants' inadequate data security measures.

79. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

80. Plaintiff provided her PII to Defendants with the reasonable expectation and mutual understanding that Defendants would use reasonable measures to protect her PII, in accordance with state and federal law and the data security promises posted on Defendants' public-facing website.

81. Since learning of the Data Breach, Plaintiff has been required to spend her valuable time and effort taking steps to avoid potential scams attempting to gain access to her accounts and mitigate the risk of misuse of her PII. Specifically, Plaintiff has been required to spend her valuable

time and effort monitoring her financial and credit monitoring accounts. Plaintiff would not have had to engage in these time-intensive efforts but for the Data Breach.

82. Plaintiff has suffered actual injury from having her PII exposed and/or stolen as a result of the Data Breach, including: (a) mitigation efforts to prevent scammers accessing her account; (b) mitigation efforts to prevent the misuse of her PII; (c) damages to and diminution of the value of her PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (d) loss of privacy.

83. Given the nature of the information compromised in the Data Breach and the propensity of criminals to use such information to commit a wide variety of crimes, Plaintiff faces a significant, present, and ongoing risk of scams, identity theft and fraud, and other identity-related fraud now and into the indefinite future.

84. In addition, knowing that hackers have gained access to her PII and that this information likely has been and will be used in the future for scams, identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

CLASS ACTION ALLEGATIONS

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

86. The class and subclass that Plaintiff seeks to represent are defined as follows:

Nationwide Class. All individuals residing in the United States and its territories, whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach, including all persons who were sent notices by Defendants that their Private Information was compromised as a result of the Data Breach.

California Subclass. All residents of California, whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach, including all California residents who were sent notices by Defendants that their Private Information was compromised as a result of the Data Breach.

87. The above-defined Nationwide Class and California Subclass are collectively referred to herein as the "Class". Excluded from the proposed Class are Defendants, their

subsidiaries and affiliates, their officers, directors, and members of their officers' and directors' immediate families, any entity in which Defendants have a controlling interest, the legal representatives, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of those judicial officers' immediate families.

88. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

89. **Numerosity.** The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including, but not limited to, the files implicated in the Data Breach. Upon information and belief, the Class, at minimum, comprises over a million individuals.

90. **Commonality.** This action involves questions of law and fact that are common to Plaintiff and the Class members. Such common questions include, but are not limited to:

- whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class members;
- whether Defendants were negligent in collecting and storing Plaintiff's and Class members' PII;
- whether Defendants had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;
- whether Defendants took reasonable steps and measures to safeguard Plaintiff's and Class members' PII;
- whether Defendants failed to adequately safeguard the PII of Plaintiff and Class members;
- whether Defendants breached their duties to exercise reasonable care in handling Plaintiff's and Class members' PII;
- 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;
- whether Plaintiff and Class members are entitled to damages as a result of Defendants' wrongful conduct; and
- whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

91. **Typicality.** Plaintiff's claims are typical of the claims of the Class members. The claims of Plaintiff and Class members are based on the same legal theories and arise from the same failure by Defendants to safeguard their PII. Plaintiff and Class members entrusted Defendants with their PII, and it was subsequently accessed by an unauthorized third party.

92. **Adequacy of Representation.** Plaintiff is an adequate representative of the proposed Class because her interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the proposed Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

93. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the proposed Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

94. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the proposed Class. If Defendants breached their duties and released Plaintiff's and Class members' PII, then Plaintiff and each Class member suffered damages by that conduct.

95. **Ascertainability.** Members of the proposed Class are ascertainable. Class membership is defined using objective criteria, and Class members may be readily identified through Defendants' books and records.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class)

96. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

97. Defendants owed a duty under common law to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

98. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' cloud-based systems to ensure that Plaintiff's and Class members' PII in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

99. Defendants' duty to use reasonable care arose from several sources, including, but not limited to, those described below.

100. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

101. Defendants also owed a common law duty because their conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendants' conduct included their failure to adequately restrict access to their computer networks and/or servers that held individuals' PII.

102. Defendants also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks, such as the Data Breach, in the financial sector.

103. Defendants breached the duties owed to Plaintiff and Class members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies provided to customers; and (h) failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

104. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, their PII would not have been accessed, exfiltrated, and compromised by cybercriminals.

105. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered injuries including:

a. theft of their PII;

b. costs associated with requesting credit freezes;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. damages to and diminution in value of their PII entrusted to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and

i. continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class members.

106. As a direct and proximate result of Defendants' negligence, including their gross negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF

NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Nationwide Class)

107. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

108. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duties.

109. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect customers' PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of a data breach.

110. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTCA was intended to protect.

111. Moreover, the harm that has occurred is the type of harm that the FTCA was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

112. Defendants' violation of Section 5 of the FTCA constitutes negligence *per se*.

113. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered harm, including those identified in Paragraph 105 above.

114. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been harmed as described herein and above, and are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF

UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Nationwide Class)

115. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

116. Plaintiff and Class members conferred a monetary benefit on Defendants by providing them with their valuable PII.

117. Defendants knew that Plaintiff and Class members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from Plaintiff's and Class members' PII and the use of Plaintiff's and Class members' PII for business purposes.

118. Defendants failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

119. Defendants acquired the PII through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

120. If Plaintiff and Class members had known Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have agreed to the entrustment of their PII to Defendants.

121. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon them.

122. Plaintiff and Class members are without an adequate remedy at law.

123. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered injuries, including those identified above.

124. Plaintiff and Class members are entitled to restitution and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation

obtained by Defendants from their wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

FOURTH CLAIM FOR RELIEF

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Nationwide Class)

125. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

126. Plaintiff and the Class entrusted their Private Information to Defendants as a condition of purchasing products and obtaining services and/or employment from Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants, pursuant to which Defendants agreed to safeguard and protect Plaintiff's and Class Members' Private Information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached, compromised, or stolen.

127. At the time Defendants acquired the Private Information of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the Private Information and not take unjustified risks when storing the Private Information.

128. Implicit in the agreements between Plaintiff and Class Members and Defendants was Defendants' obligation to: (a) use Plaintiff and Class Members' Private Information for business purposes only; (b) take reasonable steps to safeguard their Private Information; (c) prevent unauthorized access and disclosure of the Private Information; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; and (e) retain the Private Information only under conditions that kept such information secure and confidential.

129. Plaintiff and the Class would not have entrusted their Private Information to Defendants had they known that Defendants would not encrypt sensitive data elements, or delete the Private Information that Defendants no longer had a reasonable need to maintain.

130. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

131. Defendants breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their Private Information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that their Private Information had been compromised and stolen in the Data Breach.

132. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and Class Members have already suffered, and will continue to suffer, damages including, *inter alia*: (i) invasion of privacy; (ii) theft of their Private Information; (iii) actual and attempted misuse of the Private Information stolen in the Data Breach, including an increase in spam and phishing calls, texts, and emails; (iv) lost time, money, and opportunity costs associated with attempts to mitigate the actual consequences of the Data Breach; (v) lost or diminished value of their Private Information; (vi) loss of the benefit of their bargain; (vii) nominal damages; and (viii) the increased and continuing risk to their Private Information, which: (a) remains unencrypted and vulnerable to unauthorized access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

133. Plaintiff and the Class have suffered (and will continue to suffer): an ongoing and imminent threat of future identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual and attempted identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of their stolen Private Information; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, lost work time; and other economic and non-economic harm.

134. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages, in an amount to be determined at trial.

FIFTH CLAIM FOR RELIEF

VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

(On Behalf of Plaintiff and the California Subclass)

135. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

136. Plaintiff brings this claim on behalf of herself and members of the California Subclass.

137. Defendants are Businesses, as defined in Cal. Civ. Code § 1798.140.

138. Plaintiff and California Subclass members are Consumers, as defined in Cal. Civ. Code § 1798.140.

139. Defendants collected their Consumers' Personal Information, as defined in Cal. Civ. Code § 1798.140.

140. Pursuant to § 1798.150 of the CCPA, Defendants had a duty to Plaintiff and the California Subclass members to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." By failing to protect Plaintiff and the California Subclass members' Personal Information from theft, exfiltration, or unauthorized disclosure, Defendants breached their duties to implement and maintain appropriate data security procedures practices and violated § 1798.150 of the CCPA.

141. Defendants' actions directly and proximately caused Plaintiff and California Subclass members' Personal Information, including their Social Security Numbers, to be exfiltrated, stolen, disclosed, or subjected to unauthorized access.

142. In accordance with § 1798.150 of the CCPA, Plaintiff and California Subclass members seek statutory or actual damages that are a result of the Data Breach, and injunctive or declaratory relief to enjoin Defendants from continuing to violate the CCPA.

143. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages, in an amount to be determined at trial.

SIXTH CLAIM FOR RELIEF

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW ("UCL")

(On Behalf of Plaintiff and the California Subclass)

144. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

145. Plaintiff brings this claim on behalf of herself and members of the California Subclass.

146. The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code 17200.

147. Defendants' misconduct alleged herein that resulted in the Data Breach, constitutes an unlawful and unfair business practice in violation of the UCL. Prior to the Data Breach, Defendants failed to inform their customers such as Plaintiff and the other California Subclass members, that they failed to establish and maintain reasonable policies and procedures required to adequately protect the Personal Information of Plaintiff and California Subclass members.

148. Defendants' unlawful and unfair business practices are continuing, causing further harm to Plaintiff and California Subclass members.

149. Defendants' unfair and unlawful conduct directly and proximately caused harm to Plaintiff and California Subclass members, including the harm described above at Paragraph 105.

150. Plaintiff and California Subclass members seek restitution for the moneys wrongfully acquired by Defendants' unfair and unlawful practices. Plaintiff and California Subclass members also seek injunctive relief to enjoin Defendants from continuing their unlawful and unfair business practices. Plaintiff and California Subclass members further seek injunctive relief requiring Defendants to implement and maintain appropriate data security practices, in accordance with their statutory and common law duties.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, pray for relief as follows:

A. For an order certifying the proposed Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

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

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; an

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all claims so triable.

Respectfully submitted,

Dated: October 23, 2025

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
pbrown@bholaw.com
toreardon@bholaw.com
abucci@bholaw.com

NUSSBAUM LAW GROUP, P.C.
LINDA P. NUSSBAUM (*pro hac vice forthcoming*)
TANYA KORKHOV (*pro hac vice forthcoming*)
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Tel: 917/438-9189
lnussbaum@nussbaumpc.com
tkorkhov@nussbaumpc.com

CRIDEN & LOVE, P.A.
MICHAEL E. CRIDEN (*pro hac vice forthcoming*)
LINDSEY C. GROSSMAN

(*pro hac vice forthcoming*)
2020 Salzedo Street, Suite 302
Coral Gables, Florida 33134
Tel: 305/357-9000
mcriden@cridenlove.com
lgrossman@cridenlove.com

Attorneys for Plaintiff and the Proposed Class