Patrick R. Carey (Bar No. 308623)
LEXINGTON LAW GROUP, LLP
503 Divisadero Street
San Francisco, CA 94117
Telephone: 415-913-7800
Facsimile: 415-759-4112
pcarey@lexlawgroup.com

Attorneys for Plaintiff

[Additional counsel on signature page]

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

CODY SHAW, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PROSPER FUNDING LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Cody Shaw ("Plaintiff") brings this Class Action Complaint, on behalf of himself and all others similarly situated, against Defendant Prosper Funding LLC ("Defendant" or "Prosper"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against Defendant Prosper for its failure to take reasonable measures to properly secure and safeguard Plaintiff's and other similarly situated individuals ("Class Members") personally identifying information, including Social Security numbers (collectively "PII" or "Private Information") from cybercriminals.[1]

2. Prosper Funding LLC is a company that operates an online peer-to-peer lending platform connecting individual and institutional investors with consumer borrowers.

3. Plaintiff and Class Members are individuals who were required to indirectly and/or directly provide Defendant with their Private Information. By collecting, storing, and maintaining Plaintiff's and Class Members' Private Information, Prosper has a resulting duty to secure, maintain, protect, and safeguard the Private Information that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

4. Despite Prosper's duty to safeguard the Private Information of Plaintiff and Class Members, their Private Information in Defendant's possession was compromised when an unauthorized party gained access to Defendant's cloud storage platform and exfiltrated sensitive data stored therein on or about September 1, 2025 (the "Data Breach").[2]

5. The Data Breach occurred when cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive Private Information that was being kept.

---

[1] *See Form 8-K*, SEC (Sept. 17, 2025), https://www.sec.gov/Archives/edgar/data/1542574/000141626525000038/prosper-20250901.htm [https://perma.cc/N4EC-4W6M].

[2] *Id*.

6. After Prosper discovered the Data Breach in or around September 2025, it conducted an investigation which determined that its customers' data may have been acquired by cybercriminals on September 1, 2025.[3]

7. In particular, Prosper admitted in a published FAQ page on its website that it had "evidence that confidential, proprietary, and personal information, including Social Security Numbers, was obtained, including through unauthorized queries made on Company databases that store customer and applicant data."[4]

8. Although Prosper did not identify all of the types of customer data or disclose the number of persons whose information was stolen through the breach, a report by Bleeping Computer indicated that the number of persons impacted by this breach is over 17.6 million.[5] Bleeping Computer further stated that the stolen information included "customers' names, government-issued IDs, employment status, credit status, income levels, dates of birth, physical addresses, IP addresses, and browser user agent details."[6]

9. Although Defendant claims to have discovered the breach as early as September 1, 2025, Defendant did not inform victims of the Data Breach until on or around September 17, 2025. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until Defendant informed them of it.

10. Prosper failed to adequately protect the Private Information of Plaintiff and Class Members. As a result of Prosper's negligence or reckless actions, the Private Information maintained on Prosper's computer systems and network was maintained in a condition that left is vulnerable to cyberattacks.

---

[3] *Id.*

[4] *Cybersecurity Incident Customer FAQs*, PROSPER, https://www.prosper.com/legal/incident-response [https://perma.cc/5TRT-GLE7] (last visited October 20, 2025).

[5] Sergiu Gatlan, *Have I Been Pwned: Prosper data breach impacts 17.6 million accounts*, BLEEPING COMPUTER (Oct. 16, 2025), https://www.bleepingcomputer.com/news/security/have-i-been-pwned-warns-of-prosper-data-breach-impacting-176-million-accounts/ [https://perma.cc/72XP-YZ7F].

[6] *Id.*

11. Prosper knew or should have known that the failure to properly maintain adequate data security measures could result in the improper disclosure of Plaintiff's and Class Members' Private Information, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

12. Defendant disregarded its responsibilities to Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Private Information was safeguarded, failing to take available steps to prevent unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

13. As a result, Plaintiff's and Class Members' Private Information was compromised and accessed by an unauthorized third-party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

14. As a direct and proximate result of Defendant's failure to implement and follow security procedures, Plaintiff's and Class Members' Private Information is now in the hands of cybercriminals.

15. Plaintiff and Class Members have been injured by the Data Breach and are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members have been and will be required to devote time, money, and energy to protect their Private Information and themselves, to the extent possible, from future crimes.

16. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, breach of implied contract, unjust enrichment and declaratory judgment arising from the Data Breach. Plaintiff seeks damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard the Private Information in Defendant's custody to prevent

incidents like the Data Breach from reoccurring in the future, and for Defendant to provide identity theft protective services to Plaintiff and Class Members for their lifetimes.

PARTIES

17. Plaintiff Cody Shaw is an adult, who at all relevant times, was a resident and citizen of Seattle, Washington. Plaintiff's Private Information was exposed and compromised during the Data Breach.

18. Plaintiff has suffered actual injury from having his Private Information exposed and/or stolen as a result of the Data Breach, including: (a) required mitigation efforts, including researching the Data Breach and needing to monitor his financial statements to ensure his information is not used for identity theft and fraud; (b) damages to and diminution of the value of his Private Information, a form of intangible property that loses value when it falls into the hands of criminals; (c) loss of privacy; and (d) continuous imminent and impending injury raising from increased risk of financial identity theft and fraud.

19. As a result of the Data Breach, and the sensitivity of the Private Information compromised, Plaintiff will continue to be at a substantial and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

20. Defendant Prosper Funding LLC is a Delaware limited liability company with its principal executive office located at 221 Main Street, 3rd Floor, San Francisco, California 94105. According to the Form 10-Q Report for the period ending March 31, 2025 filed with the United States Securities and Exchange Commission, Prosper Funding LLC was formed in the state of Delaware in February 2012 as a limited liability company with Prosper Marketplace, Inc. ("PMI"), also located at located at 221 Main Street, 3rd Floor, San Francisco, California 94105, as its sole equity member.[7]

JURISDICTION AND VENUE

[7] Prosper Funding LLC, Q1 2025 Form 10-Q, Prosper, https://www.prosper.com/Downloads/Legal/Q1%202025%2010-Q%203.31.2025.pdf (last visited Oct. 21, 2025) [https://perma.cc/G7FS-AME4].

21. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.[8]

22. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

23. Pursuant to 28 U.S.C. §1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District, and Defendant resides in this District.

24. Divisional Assignment (L.R. 3-2 (c), (d) & (e) and 3-5(b)): A substantial part of the events which gave rise to the claims asserted herein occurred in San Francisco County where Defendant maintains its principal executive office.

FACTUAL BACKGROUND

25. Founded in 2005, Prosper represents on its website that Defendant "introduced U.S. consumers to an innovative approach to personal finance called peer-to-peer lending. Since then, we've helped over 1.7 million people access more than $27 billion in loans."[9]

26. Prosper operates an online peer-to-peer lending platform through which individual and institutional investors may fund unsecured consumer loans. Prosper facilitates these lending transactions by evaluating borrower applications, assigning credit ratings, and servicing loans on behalf of investors.

27. Plaintiff and Class Members are and/or were customers of Defendant.

---

[8] *See* 28 U.S.C. §1332(d)(10) (stating that for purposes of CAFA jurisdiction, an unincorporated association deemed to be citizen of State where it has its principal place of business and under whose laws it is organized).

[9] *About*, PROSPER, https://www.prosper.com/about (last visited Oct. 21, 2025) [https://perma.cc/G6YH-79F7].

28. As a condition of obtaining Defendant's services, Plaintiff and Class Members directly or indirectly entrusted Prosper with their sensitive Private Information.

29. Plaintiff and Class Members value the confidentiality of their Private Information and, accordingly, have taken reasonable steps to maintain the confidentiality of their Private Information.

30. In entrusting their Private Information to Defendant, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information.

31. By obtaining, collecting, and storing Plaintiff's and Class Members' Private Information, Prosper assumed equitable and legal duties to safeguard Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

32. Despite these duties, Prosper failed to implement reasonable data security measures to protect Plaintiff's and Class Members' Private Information and ultimately allowed threat actors to breach its computer systems and exfiltrate Plaintiff's and Class Members' Private Information stored therein.

I. THE VALUE OF PRIVATE INFORMATION AND EFFECTS OF UNAUTHORIZED DISCLOSURE

33. Prosper understood that the Private Information it collects was highly sensitive and of significant value to those who would use it for wrongful purposes.

34. Prosper also knew that a breach of its computer systems, and exposure of the Private Information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

35. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

36. Private Information has considerable value and constitutes an enticing and well-known target for hackers. Hackers can easily sell stolen data as there has been "proliferation of

open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[10]

37. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[11]

38. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individual, businesses, and government entities in the United States. In 2023 alone, there were 6,077 recorded breaches exposing more than 17 billion records - representing a 19.8% year-over-year increase in the United States compared to 2022.[12] This trend is mirrored in identity theft complaints, which nearly doubled over a four-year span—from 2.9 million reports in 2017 to 5.7 million in 2021.[13]

39. Indeed, a 2022 poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[14]

40. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, 2024 had the second-highest number of

---

[10] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ [https://perma.cc/7EEF-35V4].

[11] *What To Know About Identity Theft*, FTC Consumer Advice (Sept. 2024), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft [https://perma.cc/67QX-SHXV].

[12] *2024 Global Threat Intelligence Report*, FLASHPOINT (Feb. 29, 2024), https://go.flashpoint.io/2024-global-threat-intelligence-report-download [https://perma.cc/4TR4-XF8S].

[13] *Facts & Statistics: Identity Theft and Cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 [https://perma.cc/J6NE-ZCVY] (last visited October 20, 2025).

[14] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 [https://perma.cc/C79T-X7V6].

data compromises in the United States in a single year since such instances began being tracked in 2005.[15]

41. The ramifications of Prosper's failure to keep Plaintiff's and Class Members' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n 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 [Dark] 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."[16]

42. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained Private Information about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

43. The specific types of personal data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and other Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

44. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security Numbers cannot be easily replaced. Even when such numbers are replaced, the process

---

[15] *Facts + Statistics: Identity Theft and Cybercrime*, n. 13.

[16] *Report to Congressional Requesters, Personal Information, June 2007*, U.S. Gov't Accountability Office, https://www.gao.gov/new.items/d07737.pdf [https://perma.cc/QS58-NX2K] (last visited October 20, 2025).

of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

45. Indeed, the Social Security Administration warns that the process of replacing a Social Security Number is a difficult one that creates other types of problems, and that it will not be a complete remedy for the affected person:

> You should know that other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new [Social Security Number], you shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[17]

46. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of Private Information to steal and then sell.

47. Based on the value of Plaintiff's and Class Members' Private Information to cybercriminals, Prosper knew or should have known the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its data security systems were

[17] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf [https://perma.cc/DY26-AJPM].

breached. Prosper failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

II. PROSPER BREACHED ITS DUTY TO PROTECT PLAINTIFF'S AND CLASS MEMBERS' PRIVATE INFORMATION

48. On or about September 1, 2025, Prosper became aware of a cybersecurity event impacting its systems. Following the discovery of the incident, Defendant began an investigation to discover the scope of the suspicious activity.

49. Defendant's investigation confirmed that an unauthorized third-party had gained access to Defendant's systems and successfully exfiltrated Private Information stored therein. The Private Information exfiltrated in the Data Breach includes individuals, names and Social Security Numbers.

50. On or around September 17, 2025, Prosper filed a Form 8-K with the U.S. Securities and Exchange Committee ("SEC"), reporting the Data Breach and acknowledging that it had compromised the Private Information of individuals.[18]

51. Defendant's filing with the SEC acknowledged that, although the Data Breach occurred on September 1, 2025, Defendant was "still in the process of identifying what information, including the number of records of personal information, was compromised," and "ha[d] yet to determine the full scope and impact of the incident."[19]

52. Defendant also stated that it had taken steps to respond to the Data Breach but failed to provide sufficient information on how the breach occurred, what safeguards have been taken since then to safeguard further attacks, and/or where the hacked information exists today.

53. Based on Defendant's description of the Data Breach, the cyberattack was designed to gain access to private and confidential data of specific individuals, including (among other things) the Private Information of Plaintiff and the Class Members and that the cybercriminals were successful in exfiltrating sensitive information from Defendant's systems.

---

[18] *Form 8-K*, n. 1.

[19] *Id*.

54. Upon information and belief, the Private Information of approximately thousands individuals was compromised in the Data Breach.

55. The Data Breach occurred as a direct result of Prosper's failure to implement and follow basic security procedures to protect its current and former customers' Private Information that it had collected and stored.

III. PROSPER FAILED TO COMPLY WITH FTC GUIDELINES

56. Prosper is prohibited by the Federal Trade Commission Act, 15 U.S.C. §45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

57. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

58. Among other guidance, the FTC recommends the following cybersecurity guidelines for businesses in order to protect sensitive information in their systems: [21]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a

[20] *Start with Security—A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/X93U-QMDC].

[21] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf [https://perma.cc/B5US-MRRL] (last visited October 20, 2025).

business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications - the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls -settings that determine which devices and traffic get through the firewall - to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

59. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private 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.[22]

60. 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 FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[22] *Id.*

61. Prosper failed to properly implement basic data security practices. Prosper's failure to employ reasonable and appropriate measures to protect against unauthorized access to its customers' Private Information constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

62. Prosper was at all times fully aware of its obligations to protect the Private Information of its customers given the reams of Private Information that it had access to as Plaintiff's and the Class Members' servicer. Prosper was also aware of the significant repercussions that would result from a failure to properly secure the Private Information it maintained.

IV. PROSPER'S FAILURE TO PREVENT, IDENTIFY, AND TIMELY REPORT THE DATA BREACH

63. Prosper admits that an unauthorized third-party accessed its information technology system and that Defendant discovered this unauthorized access on or about September 1, 2025.[23]

64. Prosper failed to take necessary precautions and failed to employ adequate measures necessary to protect its computer systems against unauthorized access and keep Plaintiff's and Class Members' Private Information secure.

65. The Private Information that Prosper allowed to be exposed in the Data Breach is the type of private information that Prosper knew or should have known would be the target of cyberattacks.

66. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[24] Prosper failed to disclose that its systems and security practices were inadequate to reasonably safeguard individuals' Private Information.

---

[23] *Form 8-K*, n. 1.

[24] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business [https://perma.cc/JXL9-TXAK].

67. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[25] Immediate notification to individuals impacted by a data breach is critical so that those impacted can take measures to protect themselves.

68. Here, Prosper inexcusably waited several weeks after the Data Breach occurred to notify impacted individuals.

69. Plaintiff and Class Members remain in the dark regarding precisely what data was stolen, the particular malware used, and what steps are being taken to secure their Private Information in the future. Thus, Plaintiff and Class Members are left to speculate as to where their Private Information ended up, who has used it, and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

V. PLAINTIFF AND CLASS MEMBERS SUFFERED DAMAGES

70. The ramifications of Prosper's failure to keep Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

71. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

72. Private Information remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200,

[25] *Id.*

and bank details have a price range of $50 to $200.[26] "Fullz" packages, which includes "extra information about the legitimate credit card owner in case" the scammer's "bona fides are challenged when they attempt to use the credit card" are also offered on the dark web.[27]

73. Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information as a result of the Data Breach. From a recent study, 28% of individuals affected by a data breach become victims of identity fraud - this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[28]

74. Further, Plaintiff and Class Members have incurred and will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

75. Besides the monetary damage sustained in the event of identity theft, consumers may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[29]

76. Plaintiff and Class Members are also at a continued risk because their information remains in Prosper's systems, which the Data Breach showed are susceptible to compromise and attack and are subject to further attack so long as Prosper fails to take necessary and appropriate security and training measures to protect the Private Information in its possession.

---

[26] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (Apr. 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ [https://perma.cc/H9YA-DYCF].

[27] *Id*.

[28] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud [https://perma.cc/RDM7-GUFA] (last visited October 20, 2025).

[29] Cepeda Cheeks & Cassidy McCants, *How to Report identity Theft*, CONSUMERAFFAIRS (Feb. 17, 2022, updated July 25, 2023), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html [https://perma.cc/77WS-C5NJ].

77. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their Private Information to strangers.

78. As a result of Prosper's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable Private Information; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their Private Information being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their Private Information; and continued risk to Plaintiff's and the Class Members' Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Prosper fails to undertake appropriate and adequate measures to protect the Private Information entrusted to it.

79. Upon information and belief, Defendant has offered a limited subscription for identity theft monitoring and identity theft protection to impacted individuals, inadequate to Plaintiff and Class Members who will likely face many years of identity theft.

80. Such services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

CLASS ALLEGATIONS

81. Plaintiff brings this class action on behalf of himself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

82. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States and its territories whose Private Information was compromised in the Data Breach (the "Class").

83. Excluded from the Class are Prosper, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

84. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

85. **Numerosity:** Plaintiff is informed and believes, and thereon alleges that there are, at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

86. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant owed a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant actions constituted implied breaches of contract;

c. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' Private Information, and breached its duties thereby;

d. Whether Defendant was grossly negligent in collecting and storing Plaintiff's and Class Members' Private Information, and breached its duties thereby;

e. Whether Plaintiffs and other Class Members are entitled to relief under the Declaratory Judgment Act;

f. Whether Twitter caused Plaintiffs' and Class Members' injuries;

g. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

h. Whether Plaintiff and Class Members are entitled to damages, including restitution, monetary, equitable, injunctive, and other appropriate relief as a result of Defendant's wrongful conduct; and

i. Whether Defendant was unjustly enriched.

87. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all customers of Defendant, and each had their Private Information exposed and/or accessed by an unauthorized third-party.

88. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

89. **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 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.

90. **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, Defendant's liability and the fact of damages are common to Plaintiff and each member of the

Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

91. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

92. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

93. Plaintiff re-alleges the above allegations as if fully set forth herein.

94. Plaintiff and Class Members provided their Private Information to Defendant as a condition of obtaining services from Defendant.

95. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in securing, safeguarding, storing, and protecting the Private Information collected from them from being compromised, lost, stolen, accessed and misused by unauthorized parties. This duty includes, among other things, designing, maintaining, overseeing, and testing Defendant's security systems to ensure that Private Information in Prosper's possession was adequately secured and protected.

96. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

97. Defendant owed a duty of care to Plaintiff and Class Members to provide reasonable security, consistent with industry standards, to ensure that its systems and networks adequately protected their Private Information.

98. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff and Class Members' willingness to entrust Prosper with their Private Information as a condition of receiving resources was predicated on the understanding that Prosper would take adequate security precautions to protect their Private Information.

99. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

100. Plaintiff and members of the Class entrusted Defendant with their Private Information with the understanding that Prosper would safeguard their information.

101. Defendant's conduct also created a foreseeable risk of harm to Plaintiff and Class Members by failing to: (1) secure its systems and exercise adequate oversight of its data security protocols; (2) ensure compliance with industry standard data security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent the Data Breach.

102. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information, the vulnerabilities of its systems, and the importance of adequate security. Defendant should have been aware of numerous, well-publicized data breaches in the months and years preceding the Data Breach.

103. Defendant breached its common law duty to act with reasonable care in collecting and storing the Private Information of its customers, which exists independently from any contractual obligations between the parties. Specifically, Defendant breached its common law, statutory, and other duties to Plaintiff and Class Members in numerous ways, including by:

a. failing to adopt reasonable data security measures, practices, and protocols;

b. failing to implement data security systems, practices, and protocols sufficient to protect Plaintiff's and Class Members' Private Information;

c. storing former Plaintiff's and Class Members' Private Information longer than reasonably necessary;

d. failing to comply with industry-standard data security measures; and

e. failing to timely disclose critical information regarding the nature of the Data Breach.

104. Defendant's failure to implement and maintain adequate data security measures to protect Plaintiff's and Class Members' Private Information created conditions conducive to a foreseeable, intentional criminal act in the form of the Data Breach. Plaintiff and Class Members did not contribute to the Data Breach or the subsequent misuse of their Private Information.

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

106. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

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

108. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

109. Defendant has acknowledged that the Private Information of Plaintiff and Class Members was disclosed to unauthorized third persons as a result of the Data Breach.

110. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

111. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

112. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have and will suffer damages including, but not limited to: (i) the loss of value of their Private Information and loss of opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Prosper fails to undertake appropriate and adequate measures to protect it; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised for the rest of their lives.

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

114. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (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) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

116. In addition, Prosper had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

117. Defendant's violation of federal statutes, including the FTC Act, constitutes negligence *per se*.

118. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

119. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

120. Plaintiff re-alleges the above allegations as if fully set forth herein.

121. In connection with obtaining services from Defendant, Plaintiff and Class Members entered into implied contracts with Prosper.

122. Plaintiff and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining services from Defendant.

123. Defendant required Plaintiff and Class Members to provide their Private Information in order to obtain services from Defendant. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

124. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

125. When Plaintiff and Class Members provided their Private Information to Prosper, either directly or indirectly, as a pre-condition for services, they entered into implied contracts with Prosper.

126. Pursuant to these implied contracts, in exchange for the consideration and Private Information provided by Plaintiff and Class Members, Defendant agreed to, among other things, and Plaintiff and Class Members understood that Prosper would: (1) provide products and/or services to Plaintiff and Class Members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Private Information; and (3) protect Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards

127. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

128. Implicit in the agreement between Plaintiff and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures 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, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

129. The protection of Private Information was a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and Defendant, on the other hand. Indeed, as set forth herein, Defendant recognized its duty to provide adequate data security and ensure the privacy of its customers' Private Information with its practice of providing a privacy policy on its website.

130. Plaintiff and Class Members performed their obligations under the implied contract when they provided Defendant with their Private Information.

131. Defendant breached its obligations under its implied contracts with Plaintiff and Class Members in failing to implement and maintain reasonable security measures to protect and secure their Private Information and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class Members' Private Information in a manner that complies with applicable laws, regulations, and industry standards

132. The mutual understanding and intent of Plaintiff and Class Members on the one hand and Defendant, on the other, is demonstrated by their conduct and course of dealing.

133. On information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

134. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

135. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

136. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

137. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

138. Defendant breached the implied contracts it 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 accurate notice to them that Private Information was compromised as a result of the Data Breach

139. Defendant breached the implied contracts by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

140. Defendant's breach of its obligations of its implied contracts with Plaintiff and Class Members directly resulted in the Data Breach and the injuries that Plaintiff and Class Members have suffered from the Data Breach.

141. Plaintiff and Class Members suffered by virtue of Defendant's breach of their implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft–risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Private Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Private Information has been breached; (v) they were deprived of the value of their Private Information, for which there is a well-established national and international market; (vi) they have lost time and incurred expenses, and will incur future costs to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) they have overpaid for the services they received without adequate data security.

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

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

COUNT III
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Class)

144. Plaintiff re-alleges the above allegations as if fully set forth herein.

145. Every contract in the State of California has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

146. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

147. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and continued acceptance of Private Information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

148. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT IV
GROSS NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

149. Plaintiff re-alleges the above allegations as if fully set forth herein.

150. The foregoing allegations constitute gross negligence.

151. Defendant's conduct also constitutes gross negligence in so far as Defendant's breach of duty constitutes an extreme departure from the ordinary standard of care, because Prosper knowingly operated without data security systems sufficient to adequately secure user Private Information or to detect inappropriate or unauthorized access to user Private Information within Prosper's computer systems, including despite repeated warnings from the public as well as governmental entities of a data breach. In the course of breaching its duty to users to secure Private Information, Proper also knowingly operated in violation of the FTC Act. Taken together, the publicly available information strongly indicates that Prosper did essentially nothing to secure Plaintiffs' and Class Members' Private Information.

152. Prosper's actions in the course of breaching its duty of care to Plaintiffs and Class Members accordingly constitute an extreme departure from the ordinary standard of care and constitute gross negligence.

153. As a direct and proximate result of Prosper's gross negligence, Plaintiffs and Class Members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

154. Plaintiff re-alleges the above allegations as if fully set forth herein.

155. This count is plead in the alternative to the breach of implied contract count above.

156. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

157. Plaintiff and Class Members conferred a benefit on Defendant, whereby they provided their Private Information to Defendant in connection with receiving certain services.

158. Defendant, prior to and at the time Plaintiff and Class Members entrusted it with their Private Information, caused Plaintiff and Class Members to reasonably believe that it would keep that Private Information secure.

159. The monies Defendant was paid in its ordinary course of business included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiff's and Class Members' Private Information.

160. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

161. Defendant failed to disclose facts pertaining to its substandard information systems, or defects and vulnerabilities therein before Plaintiff and Class Members made their decisions to provide Defendant with their Private Information.

162. Defendant enriched itself by hoarding the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheap, ineffective security measures and diverting those funds to its own personal use. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

163. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members, and as a result, Defendant was overpaid.

164. Under principles of equity and good conscience, Defendant should not be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

165. Plaintiff and Class Members have no adequate remedy at law.

166. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (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) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

167. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

168. Plaintiff re-alleges the above allegations as if fully set forth herein.

169. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

170. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether Prosper is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that Prosper's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise

of his Private Information and remains at imminent risk that further compromises of his Private Information will occur in the future.

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

a. Prosper owes a legal duty to secure customers' Private Information and to timely notify impacted individuals of a data breach under the common law, and various state statutes; and

b. Prosper continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

172. This Court also should issue corresponding prospective injunctive relief requiring Prosper to employ adequate security protocols consistent with law and industry standards to protect Private Information in Prosper's data network.

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

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action, appointing Plaintiff as class representative for the Class, and appointing his counsel to represent the Class;

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

C. For equitable relief compelling Prosper to utilize appropriate methods and policies with respect to customer data collection, storage, and safety, and to disclose with specificity the types of Private Information compromised as a result of the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Prosper's wrongful conduct;

E. Ordering Prosper to pay for not less than ten years of credit monitoring services for Plaintiff and Class Members;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to Fed. R. Vic. P. 38(b), Plaintiff demands a trial by jury on all claims so triable.

Dated: October 22, 2025

Respectfully submitted,

LEXINGTON LAW GROUP, LLP

/s/ Patrick R. Carey
Patrick R. Carey (Bar No. 308623)
503 Divisadero Street
San Francisco, CA 94117
Telephone: (415) 913-7800
Facsimile: (415) 759-4112
pcarey@lexlawgroup.com

Joseph P. Guglielmo (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 24th Floor
New York, NY 10169
Tel.: 212-23-6444
Fax: 212-223-6334
jguglielmo@scott-scott.com

Anja Rusi (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Tel.: 860-537-5537
Fax: 860-537-4432
arusi@scott-scott.com

Attorneys for Plaintiff and the Proposed Class

JS-CAND 44 (Rev. 04-2025)

CIVIL COVER SHEET – for people without lawyers only

See Civil Local Rule 3-2 (amended April 28, 2025), which requires the filing of a civil cover sheet only by those unrepresented by counsel.

I. PLAINTIFF(S)

Cody Shaw, individually and on behalf of all others similarly situated

County of Residence of First Listed Plaintiff: King County, WA
Leave blank in cases where United States is plaintiff.

Attorney or Pro Se Litigant Information *(Firm Name, Address, and Telephone Number)*

Patrick R. Carey; Lexington Law Group, LLP; 503 Divisadero Street, San Francisco, CA 94117; 415-913-7800

DEFENDANT(S)

Prosper Funding LLC

County of Residence of First Listed Defendant: San Francisco, CA
Use ONLY in cases where United States is plaintiff.

Defendant's Attorney's Name and Contact Information *(if known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ U.S. Government Plaintiff
- ☐ Federal Question *(U.S. Government Not a Party)*
- ☐ U.S. Government Defendant
- ☒ Diversity

III. CAUSE OF ACTION

Cite the U.S. Statute under which you are filing: *(Use jurisdictional statutes only for diversity)*

28 U.S.C. § 1332, Class Action Fairness Act

Brief description of case: Privacy Data Breach

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT

- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY

- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY

- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY

- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY

- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS

- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS

- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER

- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY

- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR

- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION

- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY

- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS

- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY

- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS

- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 U.S.C. § 7609

OTHER STATUTES

- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ Original Proceeding
- ☐ Removed from State Court
- ☐ Remanded from Appellate Court
- ☐ Reinstated or Reopened
- ☐ Transferred from Another District
- ☐ Multidistrict Litigation–Transfer
- ☐ Multidistrict Litigation–Direct File

VI. FOR DIVERSITY CASES ONLY: CITIZENSHIP OF PRINCIPAL PARTIES

(Place an "X" in One Box for Plaintiff and One Box for Defendant)

Plaintiff	Defendant	
☐	☐	Citizen of California
☒	☐	Citizen of Another State
☐	☐	Citizen or Subject of a Foreign Country
☐	☒	Incorporated or Principal Place of Business In California
☐	☐	Incorporated and Principal Place of Business In Another State
☐	☐	Foreign Nation

VII. REQUESTED IN COMPLAINT

- ☑ Check if the complaint contains a **jury demand.**
- ☑ Check if the complaint contains a **monetary demand**. Amount:
- ☑ Check if the complaint seeks **class action** status under Fed. R. Civ. P. 23.
- ☐ Check if the complaint seeks a **nationwide injunction** or Administrative Procedure Act vacatur.

VIII. RELATED CASE(S) OR MDL CASE

Provide case name(s), number(s), and presiding judge(s).

IX. DIVISIONAL ASSIGNMENT pursuant to Civil Local Rule 3-2

(Place an "X" in One Box Only)

☒ SAN FRANCISCO/OAKLAND ☐ SAN JOSE ☐ EUREKA-MCKINLEYVILLE

DATE 10/22/2025 **SIGNATURE OF ATTORNEY OR PRO SE LITIGANT** /s/ Patrick R. Carey

Print Save As... Reset

COMPLETING THE CIVIL COVER SHEET

Complete the form as follows:

I. Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.

Attorney/Pro Se Litigant Information. Enter the firm name, address, telephone number, and email for attorney of record or pro se litigant. If there are several individuals, list them on an attachment.

II. Jurisdiction. Under Federal Rule of Civil Procedure 8(a), pleadings must establish the basis of jurisdiction. If multiple bases for jurisdiction apply, prioritize them in the order listed:

(1) *United States plaintiff*. Jurisdiction based on 28 U.S.C. §§ 1345 and 1348 for suits filed by the United States, its agencies or officers.

(2) *United States defendant.* Applies when the United States, its agencies, or officers are defendants.

(3) *Federal question*. Select this option when jurisdiction is based on 28 U.S.C. § 1331 for cases involving the U.S. Constitution, its amendments, federal laws, or treaties (but use choices 1 or 2 if the United States is a party).

(4) *Diversity of citizenship.* Select this option when jurisdiction is based on 28 U.S.C. § 1332 for cases between citizens of different states and complete Section VI to specify the parties' citizenship. Note: Federal question jurisdiction takes precedence over diversity jurisdiction.

III. Cause of Action. Enter the statute directly related to the cause of action and give a brief description of the cause. Do not cite jurisdictional statutes unless jurisdiction is based on diversity. Example: U.S. Civil Statute: 47 U.S.C. § 553. Brief Description: Unauthorized reception of cable service.

IV. Nature of Suit. Check one of the boxes. If the case fits more than one nature of suit, select the most definitive or predominant.

V. Origin. Check one of the boxes:

(1) *Original Proceedings*. Cases originating in the United States district courts.

(2) *Removed from State Court*. Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C. § 1441. When the petition for removal is granted, check this box.

(3) *Remanded from Appellate Court*. Check this box for cases remanded to the district court for further action, using the date of remand as the filing date.

(4) *Reinstated or Reopened*. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) *Transferred from Another District*. Check this box for cases transferred under Title 28 U.S.C. § 1404(a). Do not use this for within-district transfers or multidistrict litigation (MDL) transfers.

(6) *Multidistrict Litigation Transfer*. Check this box when a multidistrict (MDL) case is transferred into the district under authority of Title 28 U.S.C. § 1407.

(7) *Multidistrict Litigation Direct File.* Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

VI. Residence (citizenship) of Principal Parties. Mark for each principal party *only* if jurisdiction is based on diversity of citizenship.

VII. Requested in Complaint.

(1) *Jury demand.* Check this box if plaintiff's complaint demanded a jury trial.

(2) *Monetary demand*. For cases demanding monetary relief, check this box and enter the actual dollar amount being demanded.

(3) *Class action.* Check this box if plaintiff is filing a class action under Federal Rule of Civil Procedure 23.

(4) *Nationwide injunction.* Check this box if plaintiff is seeking a nationwide injunction or nationwide vacatur pursuant to the Administrative Procedures Act.

VIII. Related Cases. If there are related pending case(s), provide the case name(s) and number(s) and the name(s) of the presiding judge(s). If a short-form MDL complaint is being filed, furnish the MDL case name and number.

IX. Divisional Assignment. Identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated." Note that case assignment is made without regard for division in the following case types: Property Rights (Patent, Trademark and Copyright), Prisoner Petitions, Securities Class Actions, Anti-Trust, Bankruptcy, Social Security, and Tax.