Joseph W. Cotchett, Cal. Bar No. 36324
Thomas E. Loeser, Cal. Bar No. 202724
Gia Jung, Cal. Bar No. 340160
COTCHETT, PITRE & MCCARTHY, LLP
840 Malcom Road
Burlingame, CA 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577
jcotchett@cpmlegal.com
tloeser@cpmlegal.com
gjung@cpmlegal.com

[Additional Counsel appear on signature page]

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SHARNAY MOULTRIE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PROSPER FUNDING, LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Sharnay Moultrie, individually and on behalf of all others similarly situated ("Class Members"), upon personal knowledge of facts pertaining to Plaintiff and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendant Prosper Funding, LLC ("Prosper" or "Defendant").

NATURE OF THE ACTION

1. The release, disclosure, and publication of sensitive, private data can be devastating. It is not only an intrusion of privacy and a loss of control, but also a harbinger of identity theft. For victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have grave consequences for victims for years after the actual date of the breach. With the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, collect government benefits, or secure driver's licenses in the victims' names. Data breaches force victims to maintain constant vigilance over the misuse of their information.

2. Plaintiff brings this class action individually and on behalf of all other individuals who had their sensitive personally identifying information, including but not limited to names and Social Security numbers (SSN) (collectively, "PII" or "Personal Information"), disclosed to unauthorized third parties during a data breach experienced by Prosper in or around September 2025.

3. Prosper Funding, LLC is a marketplace-lending entity that enables borrowers to obtain unsecured consumer loans and investors to purchase securities tied to those loans.

4. In early September 2025, Prosper discovered a network security incident that impacted some of its systems. After further investigation, and with the help of a cybersecurity firm, Defendant discovered unauthorized access to its network on September 1, 2025. This unauthorized access resulted in "confidential, proprietary, and personal information, including Social Security numbers" being obtained by threat actors (the "Data Breach").[2]

[1] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, S.C. LAWYER (May 2014).

[2] *Cybersecurity Incident Customer FAQs*, https://www.prosper.com/legal/incident-response (last visited Oct. 21, 2025).

5. Little information has been made available by Prosper about the Data Breach. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been shared with Plaintiff and Class Members, who retain a vested interest in ensuring that their Personal Information remains protected.

6. Defendant was aware of or should have known of its data security shortcomings. It collects and maintains sensitive Personal Information about its customers, including SSNs and financial information. It requires customers to provide this highly confidential information in connection with using Prosper's products and services.

7. Despite knowing how valuable customer information is and the damage that would result from its release, Defendant failed to adequately protect Plaintiff's and Class Members' PII. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data.

8. Hackers targeted and obtained Plaintiff's and Class Members' PII because it empowers criminals to exploit and steal the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach, including Plaintiff and Class Members, will remain for their respective lifetimes.

9. Defendant's failures to ensure that its servers and systems were adequately secure fell far short of its obligations and Plaintiff's and Class Members' reasonable expectations for data privacy, jeopardized the security of Plaintiff's and Class Members' Personal Information, and exposed Plaintiff and Class Members to fraud and identity theft or the serious risk of fraud and identity theft.

10. As a result of Defendant's conduct and the resulting Data Breach, Plaintiff and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they have either suffered fraud or identity theft or face the substantial and continuing risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

11. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained.

PARTIES

12. Plaintiff Sharnay Moultrie is an adult citizen of the State of California, and resides in Antioch, California. Plaintiff was notified by email from Prosper on or about September 17, 2025, that her Personal Information was accessed and/or acquired by unauthorized third parties in the Data Breach.

13. As a result of the Data Breach, Plaintiff has had to monitor her accounts and anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

14. In or about the week of October 6, 2025, Plaintiff had two fraudulent charges totaling $47 charged to her debit card. As a result of this fraudulent activity, Plaintiff had to expend time and effort to cancel and replace her card.

15. As shown by the actual fraud that has occurred and as well document by privacy and cyber experts, a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff has a continuing interest in ensuring that her Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

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

JURISDICTION, VENUE AND DIVISIONAL ASSIGNMENT

17. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are in excess of 100 Class Members, the action is a class action in which one or more Class Members are citizens of states different from Defendant, and Defendant is not a government entity.

18. The Court has personal jurisdiction over Defendant because Defendant has a principal office in San Francisco, California, operates in California, conducts other significant business in California, and otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in California.

19. Venue properly lies in this judicial district because, *inter alia,* Defendant has a principal

place of business in this district; Defendant transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

20. Pursuant to Local Rules 3-2(c), 3-2(d), and 3-5(b), this civil action arose in San Francisco County because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in San Francisco County. Defendant operates from San Francisco County, which is its principal place of business.

FACTUAL ALLEGATIONS

A. Prosper Collects and Stores Personal Information

21. Prosper is a peer-to-peer marketplace-lending entity headquartered in San Francisco, California. Founded in 2005, Prosper facilitates lending transactions by evaluating borrower applications, assigning credit ratings, and servicing loans on behalf of investors. It routinely collects highly sensitive Personal Information in the process of providing its products and services.

22. Defendant is and was aware of the sensitive nature of the Personal Information it collects, and it acknowledges the importance of data privacy. It makes the following promises and claims about data privacy and security on its website:

a. "Ensuring that Prosper is private and safe is our highest priority."

b. "**Rigid privacy policy.** We follow very strict guidelines to protect your privacy."

c. "**Secure data center**. Your information is kept in a state-of-the-art data center. Physical access is strictly controlled and we use the latest in threat prevention technologies including the very best in firewall, VPN, antivirus, Web filtering and antispam technologies."

d. "**Secure encrypted sessions**. To protect your personal and financial information, we use SSL to encrypt your entire session from sign in to sign out. Only your valid email address and password will allow you to sign in to Prosper. You chose your own password during the registration process, and even Prosper employees will not be able to access your password."

e. "Prosper works hard to ensure a safe borrowing and lending environment for all

of our members."[3]

23. Prosper's Privacy Policy on its website makes clear that it will only share Personal Information with third parties at the direction of the customer with its consent: "Your Consent. Prosper may share your personal information with third parties at your direction or whenever you consent."[4]

24. Prosper's statements concerning privacy and data security make clear that it was aware of the need to safeguard the sensitive Personal Information entrusted to it as a necessary part of its business operations.

B. The Data Breach

25. On or about September 2, 2025, Prosper detected unauthorized activity on its systems.

26. According to public reporting, Prosper activated its cybersecurity response protocols, engaged cybersecurity experts to investigate, contain, and remediate the incident, and implemented enhanced security measures. It also notified law enforcement authorities.

27. Prosper's investigation has revealed evidence that an unauthorized party obtained confidential, proprietary, and personal information, including SSNs, through unauthorized queries on databases storing customer and applicant data. On information and belief, and given the nature of Prosper's business, the compromised data likely includes names, contact information, SSNs, government identification numbers, and other financial details.

28. Prosper disclosed the incident in a Form 8-K filed with the U.S. Securities and Exchange Commission on September 17, 2025, noting that the investigation into the full scope, including the number of affected records, was ongoing.[5]

29. Subsequent reports indicate that the breach impacted approximately 17.6 million unique email addresses and associated personal information.

30. The Personal Information stolen in the breach necessarily places affected individuals at

[3] *Privacy and Security at Prosper*, https://www.prosper.com/legal/security (last visited Oct. 21, 2025).

[4] *Prosper Privacy Policy & Federal Privacy Notice*, https://www.prosper.com/legal/privacy-policy (last visited Oct. 21, 2025).

[5] PROSPER FUNDING LLC, *Current Report* (Form 8-K) (Sept. 17, 2025), https://www.sec.gov/Archives/edgar/data/1416265/000141626525000038/prosper-20250901.htm

heightened risk of identity theft, phishing attacks, and financial fraud. As of this filing, Prosper has indicated that it "will be offering free credit monitoring as appropriate after we determine what data was affected"[6] but has provided no details about what monitoring offer it will make to impacted persons.

31. To date, Prosper has failed to take adequate steps to protect individuals affected by the Data Breach, instead putting the burden on Plaintiff and Class Members to take action to mitigate their damages. For example, on the incident FAQs page, Prosper tasks consumers with monitoring accounts for unauthorize activity and making time-consuming phone calls in the event of a concern[7]:

I believe there has been unauthorized activity in my account. Who should I contact?

Individuals should regularly monitor their accounts, and if you ever have any concerns about unauthorized activity in your account, please report security vulnerabilities or cyber-security incidents to security@prosper.com.

If you suspect unauthorized activity in your account, please contact:
Personal Loan: support@prosper.com or 866-615-6319, Monday-Friday from 6 a.m. – 5 p.m. PT
Credit Card: support@prospercards.com or 800-903-4697, Monday-Sunday from 5 a.m. – 7 p.m. PT
Home Equity: home@prosper.com or 800-954-2172, Monday-Friday from 7 a.m. – 4 p.m. PT
Investor Services: invest@prosper.com or 877-646-5922, Monday-Friday 6 a.m. – 3 p.m. PT

C. Impact of the Data Breach

32. As a result of the Data Breach, Plaintiff and Class Members had their most sensitive Personal Information accessed and acquired by cybercriminals, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, and unauthorized use of their Personal Information.

33. The actual extent, scope, and impact of the Data Breach remains uncertain. Unfortunately for Plaintiff and Class Members, the damage is already done because their sensitive Personal Information has been disclosed to unauthorized persons during the Data Breach.

34. Prosper knew or should have known that its affected systems and/or servers are unsecure and do not meet industry standards for protecting highly sensitive customer Personal Information. On

[6] *Cybersecurity Incident Customer FAQs,* https://www.prosper.com/legal/incident-response (last visited Oct. 21, 2025).

[7] *Id.*

information and belief, Prosper failed to timely make changes to its data security systems, privacy policies, and its IT systems and servers, exposing its customers' Personal Information to the risk of theft, identity theft, and fraud.

35. The Data Breach creates a heightened security concern for Plaintiff and Class Members because their SSNs, and likely their financial information and other sensitive information, was potentially disclosed. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new number, a breach victim must demonstrate ongoing harm from misuse of his or her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

36. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, SSNs "can be an identity thief's most valuable piece of consumer information."[8] TIME quotes data security researcher Jim Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[9]

37. Prosper had a duty to keep Plaintiff's and Class Members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personal Information to Prosper with the understanding that Prosper would comply with its privacy policies and protocols, the values it espouses regarding privacy (e.g., on its webpage entitled *Privacy and Security at Prosper*, discussed *supra*), and its obligations to keep such information confidential and secure from unauthorized disclosures.

38. Defendant's data security obligations were particularly important given the substantial increase in data breaches in recent years, which are widely known to the public and to anyone in Prosper's industry.

---

[8] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

[9] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

D. Theft of Personal Information Has Serious Consequences for Victims

39. Hostile attacks to obtain data are by no means new, and they should not be unexpected by business that collect and monetize consumer data.

40. Business Insider has noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[10] It is well known amongst companies that store sensitive personally identifying information that sensitive Personal Information—like SSNs, financial information, tax information, etc.—is valuable and frequently targeted by criminals.

41. These types of attacks should be anticipated by companies that store sensitive PII, like Prosper, and these companies must ensure that data privacy and security practices and protocols are adequate to protect against and prevent known and expected attacks.

42. Theft of Personal Information is serious. The Federal Trade Commission (FTC) has warned consumers that identity thieves use Personal Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[11]

43. Indeed, with access to an individual's Personal Information, criminals can do more than simply empty a victim's bank account. They can also commit all manner of fraud, including: 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 SSN to obtain government benefits; obtain lending or lines of credit; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, 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.[12]

---

[10] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[11] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Oct. 22, 2025).

[12] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Aug. 22, 2025).

44. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[13]

45. Personal Information is a valuable property right.[14] The value of sensitive Personal Information as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16]

46. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs, financial information, driver's license numbers, and other Personal Information directly on various illegal websites making the information publicly available, often for a price. This information from various breaches, including the information reportedly exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

47. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety

---

[13] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[15] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[16] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, NO. 220 at 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

48. Consumers place a high value on the privacy of sensitive data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

49. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[18]

50. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

51. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[19]

52. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Prosper Failed to Act in the Face of a Known Risk of a Data Breach

53. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendant failed to take reasonable steps to adequately protect Personal Information, leaving its clients (and potentially others) exposed to risk of fraud and

[17] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[18] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[19] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

identity theft.

54. Prosper is, and at all relevant times has been, aware that the sensitive Personal Information it handles and stores in connection with providing software services and products is highly sensitive. As a company that requires consumers to provide highly sensitive and identifying information, Prosper is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

55. Prosper was aware, or should have been aware, of regulatory and industry guidance regarding data security, and was alerted to the risk associated with failing to ensure that Personal Information was adequately secured.

56. Despite the well-known risks of hackers and cybersecurity intrusions, Defendant failed to employ adequate data security measures in a meaningful way in order to prevent breaches, including the Data Breach.

57. The security flaws inherent to Defendant's IT systems or servers run afoul of industry best practices and standards. Had Defendant adequately protected and secured its servers or systems, and the sensitive Personal Information stored therein, it could have prevented the Data Breach.

58. Despite the fact that Prosper was on notice of the very real possibility of data theft, including through a prior data breach, it still failed to make necessary changes, and permitted a massive intrusion to occur that resulted in disclosure of Plaintiff's and over 17 million other Class Members' Personal Information to criminals.

59. Defendant permitted Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

60. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[20]

61. As a result of the events detailed herein, Plaintiff and Class Members suffered harm and

[20] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 30, 2017), https://www.reuters.com/article/idUSKBN18M2BY/.

loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including, but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

62. Victims of the Data Breach have likely already experienced harms and are subject to a substantial and ongoing risk of harm, including identity theft and fraud.

63. As a result of Prosper's failure to ensure that its impacted systems and servers were protected and secured, the Data Breach occurred. As a result of the Data Breach, Plaintiff's and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

64. Plaintiff brings this action individually and on behalf of the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**
> All residents of the United States who were impacted by the Data Breach, including all persons who were sent notice by Defendant that their Personal Information was compromised as a result of the Data Breach.
>
> **California Subclass**
> All residents of California who were impacted by the Data Breach, including all persons who were sent notice by Defendant that their Personal Information was compromised as a result of the Data Breach.

65. The above-defined classes are referred to hereafter as the "Class" or "Classes." Excluded from the Class are: (1) any Judge presiding over this action, members of their immediate families, and court staff; and (2) Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant, or its parents, have a controlling interest, and its current or former officers and directors.

66. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class is reported to include over 17 million members who are geographically dispersed.

67. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class Members were injured through Defendant's uniform misconduct, and Plaintiff's claims are identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiff's claims are typical of Class Members' claims.

68. **Adequacy**: Plaintiff's interests are aligned with the Class Plaintiff seeks to represent, and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and undersigned counsel intend to prosecute this action vigorously. The Class's interests are well represented by Plaintiff and undersigned counsel.

69. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class Member's claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

70. **Commonality and Predominance**: The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant's data security practices resulted in the disclosure of Plaintiff's and other Class Members' Personal Information and the Data Breach;
- whether Defendant violated privacy rights and invaded Plaintiff's and Class Members'

privacy; and

- whether Plaintiff and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

71. Given that Defendant engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

72. **Injunctive and Declaratory Relief**: Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

CAUSES OF ACTION

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

73. Plaintiff realleges and incorporates paragraphs 1-72 as though fully set forth herein.

74. Defendant was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiff and Class Members.

75. Defendant knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiff and Class Members, and to not ensuring that its servers and systems, and the Personal Information, was secure. These risks were reasonably foreseeable to Defendant, including because Defendant has previously experienced a data breach.

76. Defendant owed duties of care to Plaintiff and Class Members whose Personal Information had been entrusted to it.

77. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate data security. Defendant had a duty to safeguard Plaintiff's and Class Members' Personal Information and to ensure that it adequately protected Personal Information. Defendant breached this duty.

78. Prosper's duty of care arises from its knowledge that its customers entrust it with the highly sensitive Personal Information that Prosper is required to (and represents that it will) handle

securely. Indeed, on its website, Prosper commits to data privacy, including "ensuring" that Prosper is "private and safe."

79. Only Prosper was positioned to ensure that its systems, servers, and services were sufficient to protect against breaches and the harms that Plaintiff and Class Members have now suffered.

80. A "special relationship" exists between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. Defendant entered a "special relationship" with Plaintiff and Class members by agreeing to accept, store, and have access to the sensitive Personal Information provided by Plaintiff and Class Members in connection with obtaining or utilizing Prosper's services.

81. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

82. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Personal Information.

83. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known it was failing to meet these duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

84. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have been harmed and face a substantial and continuing risk of harm.

85. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the California Class)

86. Plaintiff realleges and incorporates paragraphs 1-72 as though fully set forth herein.

87. Prosper provided or provides services, and Plaintiff and Class Members provided their Personal Information to Prosper as customers utilizing those services, or in otherwise transacting with Defendant.

88. In connection with their business relationship, Plaintiff and Class Members entered into

implied contracts with Prosper.

89. Pursuant to these implied contracts, Plaintiff and Class Members provided Prosper with their Personal Information. In exchange, Prosper agreed, among other things, to: (1) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Personal Information; and (2) protect Plaintiff's and Class Members' Personal Information in compliance with federal and state laws and regulations and industry standards.

90. The protection of Personal Information was a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and Prosper, on the other hand. Had Plaintiff and Class Members known that Prosper would not adequately protect its customers' Personal Information, they would not have done business with Prosper and utilized its services.

91. Plaintiff and Class Members performed their obligations under the implied contract when they provided Prosper with their Personal Information.

92. Necessarily implicit in the agreements between Plaintiff/Class Members and Defendant was Prosper's obligation to take reasonable steps to secure and safeguard Plaintiff's and Class Members' Personal Information.

93. Defendant breached its obligations under its implied contracts with Plaintiff and Class Members by failing to implement and maintain reasonable security measures to protect their Personal Information.

94. Defendant's breach of its obligations of its implied contracts with Plaintiff and Class Members directly resulted in the Data Breach.

95. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of its agreements.

96. Plaintiff and other Class Members were damaged by Defendant's breach of implied contracts because: (i) they have suffered actual harm or identity theft; (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 Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Personal Information has been breached; (v) they were deprived of the value of their Personal Information, for which there is a well-established

national and international market; (vi) they were deprived of the benefit of their bargain; and/or (vii) they lost time and money incurred to mitigate and remediate the effects of the breach, including the increased risks of identity theft they face and will continue to face.

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

97. Plaintiff realleges and incorporates paragraphs 1-72 as though fully set forth herein.

98. This claim is pleaded in the alternative to the implied contract claim.

99. Prosper has profited and benefited from the monies or fees paid and the Personal Information provided by Plaintiff and Class Members to receive services and benefits from Prosper.

100. Prosper has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiff and Class Members did not receive services of the quality, nature, fitness, or value represented by Prosper and that reasonable consumers expected.

101. Prosper has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiff and Class Members.

102. Equity and justice militate against permitting Prosper to retain these profits and benefits.

103. Plaintiff and Class Members suffered injury as a direct and proximate result of Prosper's unjust enrichment and seek an order directing Prosper to disgorge these benefits and pay restitution to Plaintiff and Class Members.

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

104. Plaintiff incorporates paragraphs 1-72 as if fully set forth herein.

105. Plaintiff and the Class have stated claims against Defendant based on negligence, breach of implied contracts and unjust enrichment.

106. Defendant failed to fulfill its obligations to provide adequate and reasonable security measures for the PII of Plaintiff and the Class, as evidenced by the Data Breach.

107. As a result of the Data Breach, Defendant's systems are more vulnerable to unauthorized

access and require more stringent measures to be taken to safeguard the PII of Plaintiff and the Class going forward.

108. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII of Plaintiff and the Class. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with their obligations, and that Defendant must implement and maintain reasonable security measures on behalf of Plaintiff and the Class to comply with their data security obligations.

COUNT V
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
CAL. CIV. CODE SECTION 1798.150, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

109. Plaintiff incorporates paragraphs 1-72 as if fully set forth herein.

110. Plaintiff brings this claim individually and on behalf of members of the California Subclass.

111. Defendant is a corporation organized or operated for the profit or financial benefit of its owners.

112. Defendant collected consumers' Personal Information as defined in Cal. Civ. Code § 1798.140.

113. By failing to protect Plaintiff and California Subclass Members' PII from theft, exfiltration, or unauthorized disclosure, Defendant breached its duties to ensure adequate data security practices and violated § 1798.150 of the CCPA.

114. Defendant has a duty to implement and maintain reasonable security measures to protect Plaintiff and California Subclass Members' PII. Defendant failed to do so.

115. Defendant's actions directly and proximately caused Plaintiff and California Subclass Members' Private Information, including actual names, usernames, emails, other contact information, payment information, and SSNs to be exfiltrated, stolen, disclosed, or subjected to unauthorized access.

116. Plaintiff and California Subclass Members seek equitable relief to ensure Defendant sufficiently secures customers' Private Information by implementing sufficient data security procedures and practices. Defendant continues to hold customers' PII. Plaintiff and California Subclass Members

have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated its inability to sufficiently safeguard their information through the Data Breach.

117. An actual controversy now exists as to whether Defendant has implemented and maintained adequate security procedures and practices under the CCPA, in relation to the nature of the information.

118. Judicial intervention on this issue is necessary and appropriate under the circumstances to prevent further data breaches of Plaintiff and California Subclass Members' PII.

119. Plaintiff and California Subclass Members seek statutory damages or actual damages, including actual financial losses that are a result of the unlawful data breach.

COUNT VI
CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

120. Plaintiff incorporates paragraphs 1-72 as if fully set forth herein.

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

122. Defendant is a "person" under the UCL, Cal. Bus. & Prof. Code § 17201.

123. Defendant violated the UCL through its unfair and unlawful business practices.

124. Under California's UCL, Cal. Bus. & Prof. Code Section 17200, *et seq.*, a business practice is "unfair" when any injury it causes outweighs any benefits provided to consumers and the injury is one that consumers themselves could not reasonably have avoided. *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

125. Defendant's failures to implement and maintain adequate security measures do not benefit consumers. Defendant implemented insufficient, ineffective, and cheap security measures. Defendant diverted the funds necessary to ensure sufficient data security to its own profits, which lead to the Data Breach. Defendant did not follow necessary protocols, policies, and procedures necessary for security and encryption in line with industry standards and requirements. Defendant concealed and omitted the material fact that they inadequately secured Plaintiff's and Subclass Members' PII. Defendant concealed and omitted the material fact that they did not fulfill their statutory obligations and common law duties for security of Subclass Members' PII.

126. Defendant was deceptive, misleading, and unreasonable, constituting an unfair business practice as interpreted by Cal. Bus. & Prof. Code Section 17200. Defendant's actions, as described herein, have resulted in harm to consumers who paid for Defendant's products and services inconsistent with reasonable expectations of data security.

127. California's UCL finds a business practice is "unlawful" when Defendant breach state or federal law and the "unfair competition law makes [these breaches] independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008). Defendant engaged in "unlawful" business practices by violating the FTC Act, 15 U.S.C. § 45, the CCPA, Cal. Civ. Code § 1798.100, and California common law.

128. Defendant's conduct, as alleged herein, is deceptive, misleading, unreasonable, and constitutes unlawful conduct. Defendant's conduct, including misrepresentations and omissions, was material because a regular consumer would be deceived about Defendant's data security standards. Defendant disregarded Plaintiff's and Subclass Members' rights. Defendant maliciously, intentionally, and knowingly violated California's Unfair Competition Law.

129. Defendant's unfair and unlawful conduct directly and proximately caused Plaintiff's and Subclass Members' injuries, including lost money or property. But for Defendant's unfair and unlawful acts, Plaintiff's and Subclass Members' harm would not have occurred, including a substantial and increased risk of identity theft, a diminished value for their personal information, and necessary time and expenses for monitoring fraudulent activity. Due to Defendant's unlawful conduct, as alleged herein, customers who entrusted their Private Information to Defendant have suffered injuries-in-fact as a result of the Data Breach.

130. Defendant's failure to enforce proper security measures violates public policy, which is designed to protect consumers' data and to ensure that organizations entrusted with such data adopt necessary security protocols. These objectives are reflected in laws such as the FTC Act, 15 U.S.C. § 45, and the CCPA, Cal. Civ. Code § 1798.100. Consumers cannot reasonably avoid the injuries that Defendant caused as alleged herein. Victims' injuries outweigh potential benefits to the Defendant. Defendant could have furthered its business interests in a manner other than this unfair conduct.

131. Plaintiff and California Subclass Members seek an order enjoining Defendant from

continuing its unlawful, deceptive, and unfair business practices. Plaintiff and California Subclass Members seek an order requiring Defendant to implement and maintain sufficient data security practices in accordance with statutory and common law duties. Plaintiff and California Subclass Members request an award for restitution for the money wrongfully acquired by Defendant's unfair and unlawful practices.

COUNT VII
CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT ("CLRA")
CAL. CIV. CODE 1750, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

132. Plaintiff incorporates paragraphs 1-72 as if fully set forth herein.

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

134. The CLRA prohibits "unfair methods of competition and unfair or deceptive acts or practices" in connection with the sale of goods. Cal. Civ. Code § 1770.

135. Defendant's unlawful conduct described herein was intended to increase sales to the consuming public and violated Section 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the products and services have characteristics and benefits, such as appropriate data security, that they do not have.

136. Defendant fraudulently deceived Plaintiff and the California Subclass by representing that its products and services have certain characteristics, benefits, and qualities which they do not have, namely data protection and security. In doing so, Defendant intentionally misrepresented and concealed material facts from Plaintiff and the California Subclass, specifically by advertising secure services when Defendant in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff and the California Subclass and depriving them of their legal rights and money.

137. Defendant's claims about the products and services led and continue to lead consumers like Plaintiff and Subclass Members to reasonably believe that Defendant has implemented adequate data security measures when Defendant, in fact, neglected system vulnerabilities that led to a data breach and enabled hackers to access customers' PII.

138. Defendant knew or should have known that adequate security measures were not in place and that consumers' PII was vulnerable to a data breach.

139. Plaintiff and the California Subclass have suffered injury-in-fact as a result of and in reliance upon Defendant's false representations.

140. Plaintiff and the California Subclass would not have purchased the products or used the services or would have paid significantly less for the products and services, had they known that their Personal Information was vulnerable to a data breach.

141. Defendant's actions as described herein were done with conscious disregard of Plaintiff and the rights of California Subclass Members, and Defendant was wanton and malicious in its concealment of the same.

142. Plaintiff and the California Subclass have suffered injury-in-fact and have lost money as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically, Plaintiff paid for products and services advertised as secure, and consequentially entrusted Defendant with PII, when Defendant, in fact, failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the California Subclass would not have purchased the products and services, or would not have provided Defendant with their PII, had they known that their Personal Information was vulnerable to a data breach.

143. Defendant should be compelled to implement adequate security practices to protect customers' PII. Additionally, Plaintiff and the members of the California Subclass lost money as a result of Defendant's unlawful practices.

144. Plaintiff and California Subclass Members seek all monetary and nonmonetary relief allowed by law including restitution; reasonable attorneys' fees and costs under California Code of Civil Procedures § 1021.5; and injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d) and other appropriate equitable relief.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and Class Members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiff and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

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

Respectfully Submitted,

Dated: October 22, 2025

By: */s/ Thomas E. Loeser*

Joseph W. Cotchett, Cal. Bar No. 36324
Thomas E. Loeser, Cal. Bar No. 202724
Gia Jung, Cal. Bar No. 340160
COTCHETT, PITRE & MCCARTHY, LLP
840 Malcom Road
Burlingame, CA 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577
jcotchett@cpmlegal.com
tloeser@cpmlegal.com
gjung@cpmlegal.com

Tina Wolfson (SBN 174806)
Robert Ahdoot (SBN 172098)
Alyssa Brown (SBN 301313)
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com
rahdoot@ahdootwolfson.com
abrown@ahdootwolfson.com

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)

SHARNAY MOULTRIE

County of Residence of First Listed Plaintiff: Contra Costa
Leave blank in cases where United States is plaintiff.

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

Thomas E. Loeser
Cotchett, Pitre & McCarthy LLP 840 Malcom Rd, Ste 200 Burlingame, CA 94010

DEFENDANT(S)

Prosper Funding, LLC

County of Residence of First Listed Defendant:
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(d)

Brief description of case: 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: 5,000,000.00
- ☑ 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).

McPhee v. Prosper Funding, LLC (3:25-cv-07947-CRB)

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/ Thomas E. Loeser