Colleen L. Fewer (SBN 323808)
BERGER MONTAGUE PC
505 Montgomery Street Suite 625
San Francisco, CA 94111
Tel. 415-376-2097
F. 215-875-4604
cfewer@bergermontague.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

BRIAN HUFF, individually and on behalf of all others similarly situated, Plaintiff, v. PROSPER FUNDING, LLC Defendant.	Case No. 3:25-cv-09162 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Brian Huff ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Prosper Funding, LLC ("Prosper," or "Defendant") and alleges as follows based on personal knowledge as to his own acts and on investigation conducted by counsel as to all other allegations:

I. INTRODUCTION

1. Data breaches are preventable and occur due to the lack of attention and resources that companies like Defendant expend on protecting the highly sensitive information they are entrusted with.

2. Plaintiff brings this class action against Defendant for its failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") and sensitive financial

information (collectively, "Personal Information" or "PI") in connection with a data security event disclosed by Defendant in or about September 2025 (the "Data Breach").

3. The Personal Information appears to have included confidential and sensitive information, including customers' names, Social Security Numbers, government-issued IDs, employment statuses, credit statuses, income levels, dates of birth, physical addresses, IP addresses, and browser user agent details.[1]

4. Defendant failed to comply with industry standards to protect information systems that contain Personal Information. Plaintiff seeks, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the Data Breach in the future.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Personal Information with which it was entrusted.

6. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Personal Information from those risks left that property in a dangerous condition.

7. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing

[1] 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/ (last visited October 22, 2025); *Prosper Confirms Data Breach Impacting 17 Million Users*, TechRepublic (Oct. 20, 2025), https://www.techrepublic.com/article/news-prosper-data-breach/ (last visited October 22, 2025).

to warn Plaintiff and Class Members of Defendant's inadequate data security; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, (9) failing to implement and execute an adequate comprehensive vender risk management (VRM) program; and (10) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

8. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Personal Information and failing to take standard and reasonably available steps to prevent the Data Breach.

9. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the Personal Information. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the Personal Information of Plaintiff and Class Members.

10. Plaintiff's and Class Members' identities are now at high risk because of Defendant's negligent conduct since the Personal Information that Defendant collected and maintained is now in the hands of data thieves.

11. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts and credit reports to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

12. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is hard evidence that the Plaintiff's and Class Members' Personal

Information was targeted, accessed, and has been misused.

13. Plaintiff and Class Members must now closely monitor their financial accounts and credit reports to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

14. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of their PII; and (f) the continued risk to their sensitive Personal Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect what it collected and maintained.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of Plaintiff and all similarly situated individuals whose Personal Information was accessed during the Data Breach.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

17. The exposure of one's Personal Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff and the Class Members' Personal Information was exactly what it should be—private. Not anymore. Now, their Personal Information is forever

exposed and unsecure.

II. PARTIES

A. Plaintiff

18. Plaintiff Huff is a citizen and resident of Texas.

B. Defendant Prosper Funding, LLC

19. Defendant Prosper is a corporation with its principal place of business located in San Francisco, California. Defendant conducts business throughout this District, and nationwide.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs. Upon information and belief, the number of Class Members is numerous, with many members of whom have different citizenship from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has personal jurisdiction because Defendant maintains its principal place of business in this District, regularly conducts business in this District, and has sufficient minimum contacts in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District and maintains Plaintiff's and Class Members' Personal Information in this District.

23. **Divisional Assignment**. Pursuant to Civ. L.R. 3-2(c), this action should be assigned to the San Francisco Division, as the claims arise from events occurring in San Francisco, where Defendant is based.

IV. FACTUAL ALLEGATIONS

A. Overview of Defendant

24. Prosper is a financial services company that provides loans, credit cards, and home equity financial products to its customers.

25. Defendant collected and stored Plaintiff's and the proposed Class Members' Personal Information on its information technology computer systems in San Francisco, California.

26. Defendant made promises and representations (from its headquarters in San Francisco, California) to individuals, including Plaintiff and Class Members, that the Personal Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained. For instance, Defendant's website states as follows: "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."[2]

27. Large companies like Defendant have an interest in maintaining the confidentiality of the Personal Information entrusted to them, and they are well aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding Personal Information in their possession.

28. This responsibility is heightened for Prosper because consumers must provide highly sensitive information, including Social Security Numbers and personal financial information, to access the financial products that Prosper offers. Prosper maintains Social Security Numbers, government-issued IDs, employment statuses, credit statuses, income levels, dates of birth, physical addresses, IP addresses, and other sensitive information that can easily be used to commit fraud if it ends up in the wrong hands.

29. Defendant represented to consumers and the public that it possesses robust security features to protect Personal Information and that it takes its responsibility to protect Personal Information seriously.

30. Plaintiff and Class Members provided their Personal Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply

[2] *Privacy and Security at Prosper*, Prosper, https://www.prosper.com/legal/security (last visited October 24, 2025).

with its obligations to keep such information confidential and secure from unauthorized access.

31. As a result of collecting and storing the Personal Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Personal Information from disclosure to third parties.

B. The Data Breach

32. Before September 2, 2025, an unauthorized third party gained access to Prosper's system.

33. As a result of this breach of Prosper's systems ("Data Breach"), the Personal Information of over 17.6 million Prosper customers and applicants in the United States was compromised.[3]

34. In its notice letters to impacted individuals sent on September 17, 2025, such as Plaintiff, Prosper stated: "We recently discovered unauthorized activity on our systems." Prosper further stated: "We have evidence that certain personal information, including Social Security Numbers, was obtained[.]"

35. Prosper promised that "we will be offering free credit monitoring as appropriate after we determine what data was affected." To date, that promise has not been fulfilled. Prosper has not provided a full accounting of the information that hackers were able to access, nor has Prosper offered any free data-monitoring services to Plaintiff or other impacted individuals.

36. Instead, Plaintiff learned of the full impact of the Data Breach from a third party who obtained a copy of the stolen data.[4] This third party confirmed that the following information had been stolen:

- Names

[3] Mathew J. Schwartz, *Prosper Market Data Breach Affects 17.6M Individuals*, Bank Info Security (Oct. 17, 2025), https://www.bankinfosecurity.com/prosper-market-data-breach-affects-176m-individuals-a-29755 (last visited October 22, 2025).

[4] Mathew J. Schwartz, *Prosper Market Data Breach Affects 17.6M Individuals*, Bank Info Security (Oct. 17, 2025), https://www.bankinfosecurity.com/prosper-market-data-breach-affects-176m-individuals-a-29755 (last visited October 22, 2025).

- Social Security Numbers
- Dates of birth
- Credit status information
- Email addresses
- Government issued IDs
- IP addresses
- Physical addresses
- Income levels
- Employment statuses
- Browser user agent details[5]

37. Defendant failed to prevent the Data Breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

38. The Personal Information that Defendant allowed to be exposed in the Data Breach are the types of private information that Defendant knew or should have known would be the target of cyberattacks.

39. The U.S. Federal Trade Commission ("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.[6] Immediate notification of a data breach is critical so that those impacted can take measures to protect themselves.

C. Plaintiff's Experience

40. Plaintiff Huff's Personal Information and other sensitive financial information was held by Prosper.

41. Prosper sent Plaintiff an email dated September 17, 2025, informing him that his

[5] *Prosper Data Breach*, Pwned https://haveibeenpwned.com/Breach/Prosper (last visited October 22, 2025).

[6] *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 (last visited October 22, 2025).

Personal Information was compromised in the Data Breach (the "Letter"). The Letter states that there was "unauthorized activity on our systems." This unauthorized activity meant that "certain personal information, including Social Security Numbers, was obtained" by unnamed actors.

42. The Letter does not offer any meaningful information about the cause of the Breach or the full scope of information that was accessed, leading to anxiety and serious unanswered questions for Plaintiff and other impacted individuals.

43. As a result of the Data Breach, Plaintiff has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent changing passwords for multiple online accounts, resetting his phone number, verifying the legitimacy of communications related to the Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred.

44. Plaintiff experienced hackers trying to access his financial and other online accounts after the Data Breach. While these hackers have not been able to access his accounts, he has received multiple notifications indicating attempted access.

45. In October 2025, Plaintiff received a fraudulent password reset request for a cryptocurrency exchange that he does not use. Also in October 2025, Plaintiff received a fraudulent password reset request for a NFT exchange that he does not use. Plaintiff has also received iCloud notifications requesting that he allow or deny a password reset for his iCloud account when he has not actually requested a password reset.

46. Plaintiff has also received notifications that hackers have attempted to remotely access his phone after the Data Breach. While these hackers have not been able to remotely access his phone, he has had to change phones in order to prevent future attempts.

47. Plaintiff is very careful about sharing his sensitive Personal Information and diligently maintains his Personal Information in a safe and secure manner. Plaintiff has never knowingly transmitted unencrypted sensitive Personal Information over the internet or any other unsecured source.

48. Plaintiff suffered lost time, annoyance, interference, and inconvenience because

of the Data Breach and has experienced lost sleep, stress, anxiety, and increased concerns for the loss of his Personal Information and privacy. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiff cannot be undone.

49. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

50. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of cybercriminals.

51. Future identity theft monitoring is not only reasonable and necessary and such services will include future costs and expenses. Defendant has yet to even offer credit monitoring services.

52. Plaintiff has a continuing long-term interest in ensuring that his Personal Information, which, upon information and belief, remains in Defendant's control, is protected, and safeguarded from future breaches.

D. Injuries to Plaintiff and Class Members

53. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff and Class members' Personal Information, Plaintiff and Class members have been injured.

54. Plaintiff and Class members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

55. In addition to the irreparable damage that may result from the theft of Personal Information, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours

clearing up the issues" and resolving the consequences of fraud in 2014.[7]

56. In addition to fraudulent charges and damage to their credit, Plaintiff and Class Members may spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

57. Additionally, Plaintiff and Class Members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their Personal Information is used, the diminution in the value or use of their Personal Information, and the loss of privacy.

E. Securing Personal Information and Preventing Breaches

58. Defendant could have prevented this Data Breach by properly securing and encrypting the Personal Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an internet-accessible environment when there was a reasonable need to do so.

59. Defendant's negligence in safeguarding the Personal Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

60. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect the Personal Information of Plaintiff and Class Members from being compromised.

61. The FTC defines identity theft as "a fraud committed or attempted using the

[7] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf. (last visited October 22, 2025)

identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

62. The ramifications of Defendant's failure to keep secure the Personal Information of Plaintiff and Class Members are long lasting and severe. Once Personal Information is stolen, particularly Social Security Numbers, fraudulent use of that information and damage to victims may continue for years.

F. The Value of PII

63. It is well known that Personal Information and Social Security Numbers are an invaluable commodity and a frequent target of hackers.

64. People place a high value not only on their Personal Information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[10]

65. People are particularly concerned with protecting the privacy of their financial account information and Social Security Numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[11] There are long-term consequences to data breach victims whose Social Security Numbers are taken and used by hackers. Even if they know their Social Security Numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless

---

[8] 17 C.F.R. § 248.201 (2013).

[9] *Id.*

[10] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf. (last visited October 22, 2025).

[11] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html. (last visited October 22, 2025).

they become a victim of Social Security Number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."[12]

66. The Personal Information of individuals 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, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

67. Social Security Numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security Number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

---

[12] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited October 22, 2025).

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

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, June 30, 2025, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. (last visited October 22, 2025).

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

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

68. What is more, it is no easy task to change or cancel a stolen Social Security Number. An individual cannot obtain a new Social Security Number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

69. Even then, a new Social Security Number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

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

71. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

72. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

73. Beyond personal identifying information like Social Security Numbers, the financial information maintained by Prosper is particularly prone to fraud. To apply for a loan, a

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

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html. (last visited October 22, 2025).

consumer needs to provide employment, credit, and income information. With this financial information and a Social Security Number in hand, fraudsters can apply for loans and other financial products in victims' names with accurate information.

74. The fraudulent activity resulting from the Data Breach may not come to light for years.

75. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

76. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiff and Class Members, including Social Security Numbers, and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

77. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

78. Defendant knew of the unique type and the significant volume of data contained in the Personal Information that Defendant stored on its networks, and, thus, the significant number of individuals who would be harmed by the exposure of the data.

---

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf. (last visited October 22, 2025).

79. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personal Information of Plaintiff and Class Members.

G. Industry Standards for Data Security

80. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[20]

81. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, Capital One, and Aflac, Defendant knew of the importance of safeguarding Personal Information, as well as of the foreseeable consequences of its systems being breached.

82. Therefore, the increase in such attacks, and the attendant risk of future attacks, were widely known to the public and to anyone in Defendant's industry, including Defendant.

83. Security standards commonly accepted among businesses that store Personal Information using the Internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

[20] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view. (last visited October 22, 2025).

84. The FTC publishes guides for businesses for cybersecurity[21] and protection of PII[22] which includes basic security standards applicable to all types of businesses.

85. The FTC recommends that businesses:

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 the business 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 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 business 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 hacker 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

[21] *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited October 22, 2025).

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

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.

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' network, the transmission should be investigated to make sure it is authorized.

86. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[23]

87. Because Plaintiff and Class Members entrusted Defendant with Personal Information, Defendant had a duty to keep the Personal Information secure.

88. Plaintiff and Class Members reasonably expect that when their Personal Information is provided to a sophisticated business for a specific purpose, that business will safeguard their Personal Information and use it only for that purpose.

89. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly

[23] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited October 22, 2025).

maintained and adequately protected its systems, it could have prevented the Data Breach.

H. CLASS ALLEGATIONS

90. This action is brought as a class action pursuant to Federal Rule of Civil Procedure 23.

91. Plaintiff brings this action on behalf of himself and the following Class:

> All United States individuals and entities whose Personal Information was compromised by Prosper as a result of the Data Breach.

92. The Class excludes the following: Defendant, its affiliates, and its current and former employees, officers and directors, and the judge assigned to this case.

93. The Class definition may be modified, changed, or expanded based upon discovery and further investigation.

94. *Numerosity*: The Class is so numerous that joinder of all members is impracticable, evidenced by the large number of individuals presently known to have been injured by Defendant's conduct. The Class is ascertainable by records in the possession of Defendant or third parties.

95. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and Class Members to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect Personal Information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' Personal Information secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class Members' PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Plaintiff and Class Members suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

j. Whether Plaintiff and Class Members are entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

96. *Typicality*: Plaintiff's claims are typical of the claims of Class Members. Plaintiff and Class Members were injured and suffered damages in substantially the same manner, have the same claims against Defendant relating to the same course of conduct, and are entitled to relief under the same legal theories.

97. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the Class and has no interests antagonistic to those of the Class. Plaintiff's counsel are experienced in the prosecution of complex class actions, including actions with issues, claims, and defenses similar to the present case.

98. *Predominance and superiority*: Questions of law or fact common to Class Members predominate over any questions affecting individual members. A class action is superior to other available methods for the fair and efficient adjudication of this case because individual joinder of all Class Members is impracticable and the amount at issue for each Class Member would not justify the cost of litigating individual claims. Should individual Class Members be required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far

fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court. There are no known difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

99. Further, Defendant's unlawful conduct applies generally to all Class Members, thereby making appropriate final equitable relief with respect to the Class as a whole.

V. CAUSES OF ACTION

COUNT I

NEGLIGENCE AND NEGLIGENCE PER SE

(On Behalf of the Class)

100. Plaintiff realleges and incorporates by reference herein all preceding paragraphs as if fully set forth herein.

101. Defendant owed a duty of care to Plaintiff and Class Members to use reasonable means to secure and safeguard the entrusted Personal Information, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class Members would be harmed by such exposure of their Personal Information.

102. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted their Personal Information with Defendant, Defendant accepted and held the Personal Information, and Defendant represented that the Personal Information would be kept secure pursuant to its data security policies. Defendant could have ensured that its data security systems

and practices were sufficient to prevent or minimize the Data Breach.

103. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("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 Personal Information. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

104. Defendant breached the aforementioned duties when it failed to use security practices that would protect Plaintiff's and Class Members' Personal Information, thus resulting in unauthorized third-party access to the Plaintiff's and Class Members' Personal Information.

105. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class Members' Personal Information within its possession, custody, and control.

106. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class Members' Personal Information was disseminated and made available to unauthorized third parties.

107. Defendant admitted that Plaintiff's and Class Members' Personal Information was wrongfully disclosed as a result of the Breach.

108. The Breach caused direct and substantial damages to Plaintiff and Class Members, as well as the possibility of future and imminent harm through the dissemination of their Personal Information and the greatly enhanced risk of credit fraud or identity theft.

109. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, including but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to

provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' Personal Information.

110. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

111. Neither Plaintiff nor the Class contributed to the Breach or subsequent misuse of their Personal Information as described in this Complaint.

112. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have been put at an increased risk of credit fraud or identity theft, and Defendant must mitigate damages by providing adequate credit and identity monitoring services.

113. Plaintiff and Class Members are entitled to damages for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year.

114. Plaintiff and Class Members are entitled to damages to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their Personal Information, including the amount of time Plaintiff and Class Members have spent and will continue to spend as a result of Defendant's negligence.

115. Plaintiff and Class Members are entitled to damages to the extent their Personal Information has been diminished in value because Plaintiff and Class Members no longer control their Personal Information and to whom it is disseminated.

COUNT II

BREACH OF IMPLIED CONTRACT

(On Behalf of the Class)

116. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

117. Defendant entered into various contracts with its clients to provide cloud-based software services to its clients.

118. These contracts are virtually identical to each other and were made expressly for

the benefit of Plaintiff and the Class, as Defendant agreed to safeguard and protect their confidential and private Personal Information and to timely and accurately notify Plaintiff and Class Members if their information had been breached and compromised.

119. Defendant acquired, stored, and maintained the Personal Information of Plaintiff and the Class.

120. Plaintiff and Class Members were required to provide, or authorize the transfer of, their Personal Information in order for Defendant to provide its services and/or to receive services from a company that uses Defendant's services.

121. Defendant solicited, offered, and invited Class Members to provide their Personal Information as part of its regular business practices. Plaintiff and Class Members accepted Defendant's offer and provided their Personal Information to Defendant and/or a company that used Defendant's services.

122. When Plaintiff and Class Members provided their Personal Information to Defendant (directly or indirectly), they entered into implied contracts with Defendant and intended and understood that Personal Information would be adequately safeguarded as part of that service.

123. Defendant's implied promise of confidentiality to Plaintiff and Class Members includes consideration beyond those pre-existing general duties owed under the FTC Act, or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

124. Defendant's implied promises include but are not limited to: (a) taking steps to ensure that any agents who are granted access to Personal Information also protect the confidentiality of that data; (b) restricting access to qualified and trained agents; (c) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (d) applying or requiring proper encryption; (e) multifactor authentication for access; (f) protecting Plaintiff's and Class Members' Personal Information in compliance with federal

and state laws and regulations and industry standards; and (g) other steps to protect against foreseeable data breaches.

125. Defendant's implied promises to safeguard Plaintiff's and Class Members' Personal Information are evidenced by representations on Defendant's website. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is further demonstrated by their conduct and course of dealing.

126. Plaintiff and the Class Members would not have entrusted their Personal Information to Defendant in the absence of such an implied contract. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Personal Information to Defendant.

127. Defendant recognized that Plaintiff's and Class Members' Personal Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

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

129. Defendant breached the implied contracts it made with its clients by failing to take reasonable measures to safeguard their Personal Information as described herein, as well as by failing to provide accurate, adequate, and timely notice to them that their Personal Information was compromised as a result of the Data Breach.

130. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages from: (i) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (ii) the loss of the confidentiality of the stolen Personal Information, (iii) the illegal sale of the compromised data on the dark web, (iv) lost work time, and (v) other economic and non-economic harms.

131. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendant to strengthen its data security systems, submit to future audits of those systems, and provide adequate long-term credit monitoring and identity theft protection services to all persons affected by the Data Breach.

COUNT III

UNJUST ENRICHMENT

(On behalf of the Class)

132. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

133. Defendant benefited from receiving Plaintiff's and Class Members' Personal Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

134. Defendant also understood and appreciated that Plaintiff's and Class Members' Personal Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

135. Plaintiff and Class Members conferred a monetary benefit upon Defendant by providing their Personal Information to Defendant. Plaintiffs and Class Members provided their Private Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, Plaintiff and Class Members were required to provide their Personal Information. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Personal Information held by Defendant.

136. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Personal Information of Plaintiff and Class Members for business purposes.

137. Defendant failed to provide reasonable security, safeguards, and protections to the Personal Information of Plaintiff and Class Members.

138. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

139. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

140. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

141. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT IV

VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

Cal. Civ. Code §§1798.100, *et seq*.

(On Behalf of the Class)

142. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

143. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA.

144. Plaintiff and Class Members are covered "consumers" under § 1798.140(g).

145. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

146. The Personal Information of Plaintiff and Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the information Defendant collects and which was impacted by the Data Breach includes:

> [a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information.

147. Defendant collects, stores, or otherwise maintains consumers' Personal Information.

148. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and Class Members' Personal Information from unauthorized access, decryption, exfiltration, theft, and/or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

149. Defendant had and has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class Members' Personal Information. As detailed herein, Defendant failed to do so.

150. As a direct and proximate result of Defendant's violation of its duty, some combination of Plaintiff's and Class Members' names with some combination of addresses and Social Security Numbers, were subjected to unauthorized access and exfiltration, theft, or disclosure.

151. As a direct and proximate result of Defendant's acts, Plaintiff and the Class were injured and lost money or property, including, but not limited to, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their Personal

Information, diminution of value of their Personal Information, stress, fear, and anxiety, nominal damages, and additional losses described above.

152. Plaintiff has complied with the requirements of California Civil Code Section 1798.150(b), which provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." On October 24, 2025, Plaintiff provided Defendant with written notice identifying Defendant's violations of Cal. Civil Code § 1798.150(a) and demanding the Data Breach be cured, pursuant to Cal. Civil Code § 1798.150(b).

COUNT V

CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")

Cal. Civ. Code §§ 1798.80, *et seq.*

(On Behalf of the Class)

153. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

154. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

155. The Personal Information of Plaintiff and the Class at issue in this lawsuit constitutes "personal information" under § 1798.80(e), hereafter "Personal Information."

156. Defendant is a business that owns, maintains, and licenses personal information within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiff and Class Members.

157. As alleged herein, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the unauthorized access, use and

disclosure of Plaintiff's and Class Members' Personal Information, in violation of § 1798.81.5(b).

158. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired, "or is reasonably believed to have been[] acquired by an unauthorized person" in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach" pursuant to the model security breach form provided in Cal. Civ. Code § 1798.82(d).

159. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.80 and was thus subject to the disclosure requirements of Cal. Civ. Code § 1798.82.

160. Because Defendant reasonably believed that Plaintiff's and Class Members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

161. Defendant failed to fully disclose material information about the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

162. By failing to notify Plaintiff and Class Members that their Personal Information had been compromised, Plaintiff and Class Members were prevented from taking appropriate, reasonable precautions to mitigate harms caused by the Data Breach.

163. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and Class Members suffered damages, as described above.

164. Plaintiff and Class Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT VI

CALIFORNIA UNFAIR COMPETITION LAW ("UCL")

Cal. Bus. & Prof. Code §§ 17200, *et seq*.

(On Behalf of the Class)

165. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

166. The servers affected by the Data Breach were controlled and managed by Defendant and held all Plaintiff's and Class Members' Personal Information.

167. Defendant meets the definition of a "person" as defined by Cal. Bus. & Prof. Code § 17201.

168. Plaintiff and Class Members each satisfy the definition of a "person" as defined by Cal. Bus. & Prof. Code § 17201.

169. Cal. Bus. & Prof. Code § 17204 provides that "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition" may file suit.

170. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

171. Defendant's "unfair" acts and practices include:

a. Failure to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' Personal Information being compromised, and subsequent harms caused to Plaintiff and Class Members.

b. Failure to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

c. Failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; California's Consumer Privacy Act (Cal. Civ. Code § 1798.150); and HITECH Act, 42 U.S.C. § 17902;

d. Failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security practices and policies, consumers could not have reasonably avoided the harms that Defendant caused; and

e. With respect to Defendant, engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82 disclosure requirements.

172. Defendant engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); and HITECH Act, 42 U.S.C. § 17902.

173. Defendant engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); and HITECH Act, 42 U.S.C. § 17902.

174. Defendant engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); California's Consumer Privacy Act (Cal. Civ. Code § 1798.150); and HITECH Act, 42 U.S.C. § 17902.

175. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' Personal Information being compromised, and subsequent harms caused to Plaintiff and Class Members;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach, unauthorized disclosure of Plaintiff's and Class Members' Personal Information, and subsequent harms;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U. S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' Personal Information being compromised, and subsequent harms caused to Plaintiff and Class Members;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC

Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150; and HITECH Act, 42 U.S.C. § 17902;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150; and HITECH Act, 42 U.S.C. § 17902.

176. Defendant's unfair and unlawful acts, e.g., failing to implement adequate security practices, harmed Plaintiff and Class Members.

177. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Class Members, about the adequacy of Defendant's data security policies and practices and ability to protect the confidentiality of consumers' Personal Information.

178. Had Defendant disclosed to consumers that it was not complying with industry standards or regulations or that its data systems were not secure and, thus, were vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

179. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

180. Defendant was entrusted with sensitive and valuable Personal Information regarding millions of consumers, including that of Plaintiff and Class Members. Defendant

accepted the critical responsibility of protecting the Personal Information but kept the inadequate state of its security controls secret from the public.

181. As a direct and proximate result of Defendant's unfair, unlawful, and/or fraudulent acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity and credit protection and repair services made necessary by the Data Breach.

182. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

183. Plaintiff and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

184. By deceptively, unfairly, and unlawfully storing, collecting, and disclosing their Personal Information, Defendant has taken money or property from Plaintiff and Class Members. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

185. Defendant was aware that businesses such as Defendant were a frequent target of sophisticated cyberattacks due to the recent increase in attacks and high market value of Personal Information, and on notice of the risks posed to consumers' Personal Information that they collected, stored, used, and transferred.

186. Defendant was on notice that its security and privacy policies and practices were wholly inadequate, including that of ensuring their vendors were compliant with industry standards and regulations, because of previous data breaches.

187. Defendant knew or should have known that its data security was insufficient to guard against those attacks, particularly, given the size of its database and the sensitivity of the Personal Information therein.

188. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VII

CALIFORNIA CONSTITUION'S RIGHT TO PRIVACY

Cal. Const., Art. I § I

(On Behalf of the Class)

189. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

190. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

191. The right to privacy in California's Constitution creates a private right of action against private and government entities.

192. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

193. Defendant violated Plaintiff's and Class Members' constitutional right to privacy by collecting, storing, and disclosing, or preventing from unauthorized disclosure their Personal Information in which they had a legally protected privacy interest, and for which they had a

reasonable expectation of privacy. Disclosure of their Personal Information was highly offensive given the highly sensitive nature of the data. Accordingly, disclosure of Plaintiff's and Class Members' Personal Information is an egregious violation of social norms.

194. Defendant intruded upon Plaintiff's and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Personal Information.

195. Plaintiff and Class Members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of Defendant's lax and inadequate security practices with respect to securely collecting, storing, and using data, as well as preventing the unauthorized disclosure of consumers' PII; (ii) Plaintiff and Class Members did not consent or otherwise authorize Defendant to disclose their Personal Information to parties responsible for the cyberattack; and (iii) Plaintiff and Class Members could not reasonably expect Defendant would commit acts in violation of laws protecting their privacy.

196. As a result of Defendant's actions, Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation.

197. Plaintiff and Class Members suffered actual and concrete injury as a result of Defendant's violations of their privacy interests. Plaintiff and Class Members are entitled to appropriate relief, including damages to compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

198. Plaintiff and Class Members seek appropriate relief for that injury, including, but not limited to, damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class Members' privacy.

COUNT VIII

INJUNCTIVE/DECLARATORY RELIEF

(On Behalf of the Class)

199. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

200. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure Personal Information.

201. Defendant still stores Plaintiff's and Class Members' Personal Information.

202. Since the Data Breach, Defendant has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

203. Defendant has not satisfied its legal duties to Plaintiff and Class Members.

204. Actual harm has arisen in the wake of the Data Breach regarding Defendant's duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Personal Information, and Defendant's failure to address the security failings that led to that exposure.

205. Plaintiff, therefore, seeks a declaration: (a) that Defendant's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. ordering that Defendant engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Defendant engage third-party security auditors and internal personnel

to run automated security monitoring;

c. ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that Defendant segment customer Personal Information by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. ordering that Defendant purge, delete, and destroy in a reasonably secure manner Personal Information not necessary for its provision of services;

f. ordering that Defendant conduct regular computer system scanning and security checks; ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

g. ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face because of the loss of their Personal Information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for a judgment as follows:

a. For an order certifying the Class, appointing Plaintiff as Class Representative, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory, punitive, statutory, and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees; and

f. Such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiff hereby respectfully demands a trial by jury.

Dated: October 24, 2025

Respectfully submitted,

/s/Colleen L. Fewer

Colleen L. Fewer (SBN 323808)
BERGER MONTAGUE PC
505 Montgomery Street, Suite 625
San Francisco, CA 94111
T. 415.376.2097
F.215.875.4604

Counsel for Plaintiff and Proposed Class

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)

Brian Huff, individually and on behalf of all others similarly situated,

County of Residence of First Listed Plaintiff: Dallas (TX)
Leave blank in cases where United States is plaintiff.

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

Berger Montague, 505 Montgomery St, Ste 625, San Francisco CA 94111

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)(2)

Brief description of case: Allegations against defendant regarding 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).

McPhee v. Prosper Funding, LLC, No. 3:25cv7947, Breyer

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 10/24/2025 **SIGNATURE OF ATTORNEY OR PRO SE LITIGANT** /s/Colleen Fewer

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.