David M. Berger (SBN 277526)
GIBBS MURA LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
Tel: (510) 350-9700
Fax: (510) 350-9701
dmb@classlawgroup.com

James J. Pizzirusso (admitted *pro hac vice*)
HAUSFELD LLP
1200 17th Street, N.W.
Suite 600
Washington, DC 20036
Tel: (202) 540-7200
Fax: (202) 540-7201
jpizzirusso@hausfeld.com

Co-Lead Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: PROSPER FUNDING, LLC DATA BREACH LITIGATION

This Document Relates To: All Parties

Lead Case No. 3:25-cv-07947-CRB

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Plaintiffs Sara Petty, Jhonny Blandino Soto, Sabrina MacDonald, Joby Childress, Brian Huff, Ada Rivera, Sharnay Moultrie, Theresa Castillo, Billy Yoder, Christopher McPhee, Elaine Bell, Heather O'Neill, Virginia Justiniano, Hunter Fast, Felicity Palma, Steven Wions, Alexander Cooper, and Helena Pappadakis ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Class Action Complaint against Defendants Prosper Funding, LLC and Prosper Marketplace, Inc. ("Prosper" or "Defendants"), alleging as follows based upon personal knowledge and the investigation of counsel.

I. NATURE OF THE ACTION

1. Prosper, a self-described "fintech pioneer"[1] whose motto is "helping people thrive,"[2] announced on September 17, 2025, that cybercriminals were able to obtain sensitive personally identifying information ("PII") associated with as many as 17.6 million people by querying the company's internal databases.[3] At the hub of Prosper's personal finance enterprise were treasure troves of PII that should have been protected by extraordinarily strict access and authentication controls, vigilant monitoring for suspicious activity, and alerting that would prompt rapid responses from Prosper's information security personnel. Although Prosper has provided very little information about its data breach, the few details available suggest Prosper allowed stunning security lapses to fester in its network environment, making a major data breach inevitable. What's more, the number of affected individuals appears to dwarf the number of loans Prosper claims to have issued by nearly tenfold,[4] suggesting that Prosper not only failed to responsibly dispose of PII for applicants who did not obtain loans or other financial services with it, but also that Prosper

[1] *Prosper Notice of Data Breach*, Prosper, https://www.prosper.com/blog/prosper-notice-of-data-breach (accessed Mar. 23, 2026).

[2] Prosper, https://www.prosper.com/ (accessed Mar. 26, 2026).

[3] Ionut Arghire, *Prosper Data Breach Impacts 17.6 Million Accounts*, Security Week (Oct. 17, 2025) https://www.securityweek.com/prosper-data-breach-impacts-17-6-million-accounts/.

[4] *About Us*, Prosper, https://www.prosper.com/about (accessed Mar. 26, 2026).

engaged in aggressive tactics to acquire PII of non-customers with little thought to data security for those individuals.

2. Plaintiffs bring this class action against Prosper for failing to properly secure and safeguard Plaintiffs' and Class Members' sensitive personally identifying information ("PII"),[5] which is now in the hands of cybercriminals as a result.

3. Due to Defendants' failure to implement reasonable or adequate data security measures, cybercriminals targeted and accessed Defendants' network systems and stole Plaintiffs' and Class Members' sensitive, confidential PII stored therein, including their full names in combination with their Social Security numbers, and other highly sensitive personal and financial data, causing widespread injuries to Plaintiffs and Class Members (the "Data Breach").

4. Plaintiffs and Class Members fall into two distinct categories. Some are current and former Prosper customers who had to entrust Prosper with their sensitive, non-public PII in order to apply for and/or obtain financial services from Prosper (the "Customer Subclass").[6] Defendants could not perform their operations or provide their services without collecting Plaintiffs' and Customer Subclass Members' PII. The massive number of records compromised in the Data Breach could only be possible if Prosper retained this PII for many years—even if Prosper's relationship with a Customer Subclass Member ended or was never finalized.

5. A second category of Plaintiffs and Class Members did not knowingly enter into a relationship with Prosper or provide Prosper with their PII but have been informed by Prosper or private monitoring organizations that their sensitive, non-public PII was exposed in the Data Breach (the "No Relationship Subclass"). Given the minimal information Prosper has provided to victims of the Data Breach, the No Relationship Subclass Members do not generally know how Prosper

[5] The Federal Trade Commission ("FTC") defines "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…." 17 C.F.R. § 248.201(b)(8).

[6] Included in the Customer Class are individuals who applied for Defendants' financial services and were required to entrust Defendants with their PII in the application process but were either not approved for those services or ultimately decided not to accept services from Defendants.

obtained their PII. And, as described further below, Prosper's business practices include acquiring PII from third parties without the data subjects' knowledge, including through referral services and as a byproduct of purchasing existing loans from other lending institutions.[7] That Prosper failed to adequately secure the information it hoarded on these unwitting subjects makes this Data Breach particularly distressing to victims.

6. Financial institutions like Defendants that handle PII owe the individuals to whom that data relates duties to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and to keep it safe and confidential. These duties arise under contract, statutory and common law, industry standards, representations made to Plaintiffs and Class Members, and because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals.

7. Defendants breached these duties owed to Plaintiffs and Class Members by failing to safeguard their PII, which it collected and maintained, including by failing to implement industry standards for data security to protect against, detect, and stop cyberattacks, which allowed criminal hackers to access and steal millions of consumers' PII.

8. While Defendants notified Plaintiffs and Class Members their PII had been compromised, Defendants' notice failed to explain when the Data Breach actually took place or provide many details of how the Data Breach occurred, diminishing Plaintiffs' and Class Members' ability to timely and thoroughly respond to the Data Breach and protect themselves or mitigate the harms the Data Breach caused them.

9. Defendants failed to adequately protect Plaintiffs' and Class Members' PII and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or reckless acts and omissions and its failure to protect its customers' sensitive data.

10. The few details that have been released about the Data Breach strongly suggest Defendants had recklessly deficient technical and administrative cybersecurity controls, particularly

[7] Prosper Marketplace, Inc., Prosper Funding LLC, Annual Report (Form 10-K) (Mar. 26, 2025).

given the massive amount of data that Defendants hoarded. The potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendants, and thus, Defendants knew that failing to take reasonable steps to secure the PII left that data in a dangerous condition.

11. Hackers targeted and obtained Plaintiffs' and Class Members' PII from Defendants' systems because that data is incredibly valuable. PII of the types taken in this Data Breach can be sold in illicit criminal networks, including on the dark web, and is frequently used to commit identity fraud and other crimes. As a direct and proximate result of Prosper's breaches of its duties to implement reasonable information security controls and manage PII with reasonable care, Plaintiffs' and Class Members' PII has been accessed and exfiltrated by hackers and exposed to an untold number of unauthorized individuals. The present and continuing risk to Plaintiffs and Class Members will remain for their respective lifetimes.

12. The harms resulting from a data breach manifest in numerous ways, including identity theft and financial fraud. The exposure of an individual's PII due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent it is possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take additional prophylactic measures.

13. As a result of the Data Breach, Plaintiffs and Class Members suffered and will continue to suffer concrete injuries in fact, 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) actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) decreased value of their PII; (g) loss of privacy and of their property right to exclude others from their PII; (h) emotional distress including anxiety and stress; and (i) the continued risk to their sensitive PII, which remains in Defendants' inadequately secured systems and subject to further breaches.

14. To remedy Defendants' inadequate safeguarding of Plaintiffs' and Class Members' PII, Plaintiffs, on behalf of themselves and the Class, bring claims for negligence, negligence *per se*, breach of contract, unjust enrichment, and violation of California's Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq*. ("UCL"). In addition, Plaintiffs Rivera, Moultrie, Castillo, McPhee, Petty, Pappadakis, and Justiniano bring statutory claims on behalf of the respective state subclasses for the following states: California, New York, Colorado, and Florida.[8]

15. Plaintiffs and Class Members seek damages and equitable relief requiring Defendants to (a) disclose the full nature of the Data Breach and types of PII exposed; (b) implement data security practices to reasonably guard against future breaches; and (c) provide, at Defendants' expense, all Data Breach victims with lifetime identity theft protection services.

II. JURISDICTION, VENUE, AND DIVISIONAL ASSIGNMENT

16. This Court has jurisdiction over this controversy under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs, there are over 100 putative Class Members, and numerous Class Members (including several Plaintiffs) are citizens of a different state than Defendant.

17. This Court has personal jurisdiction over Defendants because they are headquartered in California and regularly conduct business within this state.

18. Venue is proper in this District because Defendants' principal office is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District. Accordingly, under Local Rule 3-2, this matter should be assigned to the San Francisco Division.

[8] Pursuant to Massachusetts General Laws ("M.G.L."), chapter 93A, § 9(3), Plaintiff Blandino Soto intends to send a written demand to Defendants for relief on behalf of himself and a class of similarly situated individuals for relief from Defendants' violations of M.G.L. ch. 93A, § 2 that led to the Data Breach. Defendants have thirty days from the letter's date to make a reasonable offer of relief. If Defendants fail to make such an offer, or their offer does not adequately provide the relief sought, Plaintiffs request leave to amend their allegations to include a cause of action under M.G.L. ch. 93A. Plaintiffs also request leave to amend their allegations to include other state statutory causes of action as they obtain discovery clarifying the Defendants' relationships with Plaintiffs and other Class Members.

III. PARTIES

Defendants

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

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

Plaintiff Blandino Soto's Experience

21. Plaintiff Jhonny Blandino Soto is an individual and a citizen and resident of Essex County, Massachusetts.

22. Plaintiff Blandino Soto is a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Blandino Soto took out a personal 5-year loan with Prosper in June 2023 and continues to make payments on the loan.

23. Plaintiff Blandino Soto provided his PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Blandino Soto would not have provided his PII to Prosper had he known it would be stored using inadequate data security and left vulnerable to a cyberattack.

24. Plaintiff Blandino Soto greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff Blandino Soto diligently protects his PII and stores any documents containing PII in a safe and secure location.

25. At the time of the Data Breach, Prosper retained Plaintiff Blandino Soto's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Blandino Soto's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

26. On or about December 15, 2025, Prosper informed Plaintiff Blandino Soto that his PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiffs' sensitive PII, including his Social Security Number/National ID Number and date of birth.

27. Plaintiff Blandino Soto further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

28. Since the Data Breach, Plaintiff Blandino Soto has experienced an increase in spam text messages using his private information.

29. Plaintiff Blandino Soto has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Blandino Soto also placed a credit freeze with each of the three credit bureaus. Plaintiff Blandino Soto has spent many hours dealing with the Data Breach since learning about it, valuable time he otherwise would have spent on other activities.

30. Plaintiff Blandino Soto further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

31. Due to the Data Breach, Plaintiff Blandino Soto is at a present risk and will continue to be at risk of identity theft and fraud for years.

32. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

33. Plaintiff Blandino Soto has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

34. The Data Breach has also caused Plaintiff Blandino Soto to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

35. As a direct and traceable result of the Data Breach, Plaintiff Blandino Soto suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including:

(a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff MacDonald's Experience

36. Plaintiff Sabrina MacDonald is an individual and a citizen and resident of Oakland County, Michigan.

37. To the best of her recollection, Plaintiff MacDonald has never applied for or obtained any financial services from Prosper.

38. Plaintiff MacDonald never directly provided her PII to Prosper and is unaware of how Prosper obtained her PII. Plaintiff MacDonald suspects Prosper purchased or otherwise obtained her PII from a third party.

39. Plaintiff MacDonald greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff diligently protects her PII and stores any documents containing PII in a safe and secure location.

40. At the time of the Data Breach, Prosper retained Plaintiff MacDonald's PII in its databases and other systems. These databases and other systems were inadequately secured, which made it possible for Plaintiff MacDonald's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

41. Despite having never directly provided Prosper with her PII, on or about October 15, 2025, Plaintiff MacDonald learned her PII may have been accessed by cybercriminals in the Data Breach through a notification by the website www.haveibeenpwned.com ("Have I Been Pwned"), a reputable website that permits users to see whether their information has been compromised. Prosper has failed to provide plaintiff with any notice whatsoever. According to Have I Been

Pwned's notification, the hackers acquired files containing Plaintiff MacDonald's sensitive PII, including her government-issued IDs, date of birth, and credit status information.

42. Plaintiff MacDonald further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

43. Since the Data Breach, Plaintiff MacDonald has received fraud alerts and experienced an increase in spam phone calls and text messages.

44. Plaintiff MacDonald has made reasonable efforts to mitigate the impact of the Data Breach, including researching and monitoring the Data Breach and calling consumer protection services about any indications of actual or attempted identity theft or fraud. Plaintiff MacDonald has spent many hours dealing with the Data Breach since learning of it, valuable time she otherwise would have spent on other activities.

45. Plaintiff MacDonald further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

46. Due to the Data Breach, Plaintiff MacDonald is at a present risk and will continue to be at risk of identity theft and fraud for years.

47. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

48. Plaintiff MacDonald has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

49. The Data Breach has also caused Plaintiff MacDonald to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence, the information stolen, or how Prosper obtained Plaintiff MacDonald's PII in the first instance.

50. As a direct and traceable result of the Data Breach, Plaintiff MacDonald suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including:

(a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Huff's Experience

51. Plaintiff Brian Huff is an individual and a citizen and resident of Collin County, Texas.

52. Plaintiff Huff is a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Huff obtained a credit card from Prosper and has applied for a personal loan with Prosper.

53. Plaintiff Huff provided his PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Huff would not have provided his PII to Prosper had he known it would be stored using inadequate data security and left vulnerable to a cyberattack.

54. Plaintiff Huff greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff Huff diligently protects his PII and stores any documents containing PII in a safe and secure location.

55. At the time of the Data Breach, Prosper retained Plaintiff Huff's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Huff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

56. On or about September 17, 2025, Prosper informed Plaintiff Huff that his PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiff Huff's sensitive PII, including his Social Security Number.

57. Plaintiff Huff further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

58. Since the Data Breach, Plaintiff Huff has suffered several attempts at fraud and experienced an increase in phishing emails and spam phone calls.

59. Plaintiff Huff has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach, placing a freeze on his credit, changing account passwords, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Huff has spent many hours dealing with the Data Breach since learning about it, valuable time he otherwise would have spent on other activities.

60. Plaintiff Huff further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

61. Due to the Data Breach, Plaintiff Huff is at a present risk and will continue to be at risk of identity theft and fraud for years.

62. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

63. Plaintiff Huff has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

64. The Data Breach has also caused Plaintiff Huff to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

65. As a direct and traceable result of the Data Breach, Plaintiff Huff suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not

adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Castillo's Experience

66. Plaintiff Theresa Castillo is an individual and a citizen and resident of Los Angeles County, California.

67. Plaintiff Castillo was a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Castillo took out a personal loan with Prosper, which she has fully paid off.

68. Plaintiff Castillo provided her PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Castillo would not have provided her PII to Prosper had she known it would be stored using inadequate data security and left vulnerable to a cyberattack.

69. Plaintiff Castillo greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff diligently protects her PII and stores any documents containing PII in a safe and secure location.

70. At the time of the Data Breach, Prosper retained Plaintiff Castillo's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Castillo's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

71. On or about September 17, 2025, Prosper informed Plaintiff Castillo that her PII may have been taken by cybercriminals in the Data Breach. Prosper has failed to provide Plaintiff any update since that time that her PII was not, in fact, compromised.

72. Plaintiff Castillo further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

73. Since the Data Breach, Plaintiff Castillo has experienced a fraudulent attempt at opening a bank account in her name, using her address and Social Security Number. She has also received multiple alerts that her personal information is on the dark web.

74. Plaintiff Castillo has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach, speaking with Prosper representatives on the phone, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Castillo has spent many hours dealing with the Data Breach since learning about it, valuable time she otherwise would have spent on other activities.

75. Plaintiff Castillo further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

76. Due to the Data Breach, Plaintiff Castillo is at a present risk and will continue to be at risk of identity theft and fraud for years.

77. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

78. Plaintiff Castillo has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

79. The Data Breach has also caused Plaintiff Castillo to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

80. As a direct and traceable result of the Data Breach, Plaintiff Castillo suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft

now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Yoder's Experience

81. Plaintiff Billy Yoder is an individual and a citizen and resident of Winston County, Alabama.

82. Plaintiff Yoder is a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Yoder applied for a loan and obtained a credit card through Prosper.

83. Plaintiff Yoder provided his PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Yoder would not have provided his PII to Prosper had he known it would be stored using inadequate data security and left vulnerable to a cyberattack.

84. Plaintiff Yoder greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

85. At the time of the Data Breach, Prosper retained Plaintiff Yoder's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Yoder's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

86. On or about September 17, 2025, Prosper informed Plaintiff Yoder that his PII may have been taken by cybercriminals in the Data Breach. Prosper has failed to provide Plaintiff Yoder any update since that time that his PII was not, in fact, compromised.

87. Plaintiff Yoder further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

88. Since the Data Breach, Plaintiff Yoder has received alerts from Experian that his PII, including Social Security Number, are on the dark web. Plaintiff Yoder has also experienced an increase in spam calls, emails, and texts requesting his personal or financial information.

89. Plaintiff Yoder has made reasonable efforts to mitigate the impact of the Data Breach, including reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Yoder now monitors his financial and credit statements multiple times a week and has spent many hours dealing with the Data Breach since learning about it, valuable time he otherwise would have spent on other activities.

90. Plaintiff Yoder further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

91. Due to the Data Breach, Plaintiff Yoder is at a present risk and will continue to be at risk of identity theft and fraud for years.

92. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

93. Plaintiff Yoder has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

94. The Data Breach has also caused Plaintiff Yoder to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

95. As a direct and traceable result of the Data Breach, Plaintiff Yoder suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Wions's Experience

96. Plaintiff Steven Wions is an individual and a citizen and resident of Baltimore County, Maryland.

97. Plaintiff Wions was a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff made investments with Prosper on several occasions between 2007 and 2008. Plaintiff Wions last received a payment on these investments in 2011.

98. Plaintiff Wions provided his PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Wions would not have provided his PII to Prosper had he known it would be stored using inadequate data security and left vulnerable to a cyberattack.

99. Plaintiff Wions greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

100. At the time of the Data Breach, Prosper retained Plaintiff Wions's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Wions's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

101. On or about December 9, 2025, Prosper informed Plaintiff Wions that his PII was taken by cybercriminals in the Data Breach. According to the Notice Letter, the cybercriminals acquired files containing Plaintiffs' sensitive PII, including his Social Security Number/National ID Number.

102. Plaintiff Wions further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

103. Since the Data Breach, Plaintiff Wions has received an alert that his personal information was on the dark web.

104. Plaintiff Wions has made reasonable efforts to mitigate the impact of the Data Breach, including reviewing credit reports, fraud monitoring services, and financial account

statements for any indications of actual or attempted identity theft or fraud. Plaintiff Wions has spent multiple hours dealing with the Data Breach since learning about it, valuable time he otherwise would have spent on other activities.

105. Plaintiff Wions further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

106. Due to the Data Breach, Plaintiff Wions is at a present risk and will continue to be at risk of identity theft and fraud for years.

107. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

108. Plaintiff Wions has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

109. The Data Breach has also caused Plaintiff Wions to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

110. As a direct and traceable result of the Data Breach, Plaintiff Wions suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Cooper's Experience

111. Plaintiff Alexander Louis Cooper is an individual and a citizen and resident of Clark County, Nevada.

112. To the best of his recollection, Plaintiff Cooper has never applied for or obtained any financial services from Prosper.

113. Plaintiff Cooper never directly provided his PII to Prosper and is unaware of how Prosper obtained his PII. Plaintiff Cooper suspects Prosper purchased or otherwise obtained his PII from a third party.

114. Plaintiff Cooper greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location.

115. At the time of the Data Breach, Prosper retained Plaintiff Cooper's PII in its databases and other systems. These databases and other systems were inadequately secured, which made it possible for Plaintiff Cooper's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

116. Despite having never directly provided Prosper with his PII, on or about December 15, 2025, Prosper informed Plaintiff Cooper that his PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiffs' sensitive PII, including his Social Security Number / National ID Number and date of birth.

117. Plaintiff Cooper further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

118. Since the Data Breach, Plaintiff Cooper has been the victim of attempted financial fraud. Specifically, Plaintiff learned that an unknown individual had attempted repeatedly to purchase computer products using his payment information.

119. Plaintiff Cooper has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account

statements for any indications of actual or attempted identity theft or fraud. Plaintiff Cooper now monitors his financial statements multiple times a week and has spent many hours dealing with the Data Breach since learning of it, valuable time he otherwise would have spent on other activities.

120. Plaintiff Cooper further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

121. Due to the Data Breach, Plaintiff Cooper is at a present risk and will continue to be at risk of identity theft and fraud for years.

122. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

123. Plaintiff Cooper has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

124. The Data Breach has also caused Plaintiff Cooper to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence, the information stolen, or how Prosper obtained Plaintiff Cooper's PII in the first instance.

125. As a direct and traceable result of the Data Breach, Plaintiff Cooper suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Pappadakis's Experience

126. Plaintiff Helena Anne Pappadakis is an individual and a citizen and resident of Adams County, Colorado.

127. Plaintiff Pappadakis applied for Prosper's financial services prior to the Data Breach. Specifically, Plaintiff Pappadakis applied for a loan from Prosper around June of 2025. Plaintiff Pappadakis ultimately did not obtain any such financial services from Prosper.

128. Plaintiff Pappadakis provided her PII to Prosper when she applied for financial services from Prosper. Plaintiff Pappadakis would not have provided her PII to Prosper had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

129. Plaintiff Pappadakis greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiffs diligently protect her PII and store any documents containing PII in a safe and secure location. Plaintiff Pappadakis deletes any documents she receives that contain any PII or that may contain any information that could otherwise be used to compromise her identity and payment card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

130. At the time of the Data Breach, Prosper retained Plaintiff Pappadakis's PII in its databases and other systems. These databases and other systems were inadequately secured, which made it possible for Plaintiff Pappadakis's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

131. On or about December 17, 2025, Prosper informed Plaintiff Pappadakis that her PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiffs' sensitive PII, including her Social Security Number / National ID Number and date of birth.

132. Plaintiff Pappadakis further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

133. Since the Data Breach, Plaintiff Pappadakis has experienced an increase in spam calls and texts using her PII, including from entities impersonating the employees of the Social Security Administration or health insurance agents.

134. Plaintiff Pappadakis has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Pappadakis now monitors her financial and credit statements multiple times a week and has spent many hours dealing with the Data Breach, valuable time they otherwise would have spent on other activities.

135. Plaintiff Pappadakis further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

136. Due to the Data Breach, Plaintiff Pappadakis is at a present risk and will continue to be at risk of identity theft and fraud for years.

137. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

138. Plaintiff Pappadakis has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

139. The Data Breach has also caused Plaintiff Pappadakis to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper's still have not fully informed her of key details about the Data Breach's occurrence or the information stolen. Specifically, Plaintiff Pappadakis has experienced panic attacks resulting from her distress about the potential consequences of the Data Breach.

140. As a direct and traceable result of the Data Breach, Plaintiff Pappadakis suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now

possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Petty's Experience

141. Plaintiff Sara Petty is an individual and a citizen and resident of Westchester County, New York.

142. Plaintiff Petty is a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Petty obtained a credit card through Prosper around 2024 and also applied for a personal loan with Prosper around August of 2025.

143. Plaintiff Petty provided her PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Petty would not have provided her PII to Prosper had she known it would be stored using inadequate data security and left vulnerable to a cyberattack.

144. Plaintiff Petty greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff Petty diligently protects her PII and stores any documents containing PII in a safe and secure location.

145. At the time of the Data Breach, Prosper retained Plaintiff Petty's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Petty's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

146. On or about December 17, 2025, Prosper informed Plaintiff Petty that her PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiffs' sensitive PII, including her Social Security Number / National ID Number, date of birth, and Other Financial / Credit Application Information.

147. Plaintiff Petty further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

148. Since the Data Breach, Plaintiff Petty has experienced an increase in alerts that her personal information is on the dark web and has noticed several items on her credit report that she did not recognize. She has also seen an uptick in spam phone calls and text messages.

149. Plaintiff Petty has also been a victim of attempted financial fraud since the Data Breach began. Around July of 2025, Plaintiff Petty noticed a $74 charge on her debit card that she did not authorize. Upon investigation, the bank determined the charge was fraudulent and issued a refund. Plaintiff Petty was obligated to obtain a new debit card with a new number as a result.

150. Plaintiff Petty has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Petty now monitors her financial and credit statements multiple times a week and has spent many hours dealing with the Data Breach since learning about it, valuable time she otherwise would have spent on other activities.

151. Plaintiff Petty further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

152. Due to the Data Breach, Plaintiff Petty is at a present risk and will continue to be at risk of identity theft and fraud for years.

153. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

154. Plaintiff Petty has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

155. The Data Breach has also caused Plaintiff Petty to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

156. As a direct and traceable result of the Data Breach, Plaintiff Petty suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost

time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing their PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Moultrie's Experience

157. Plaintiff Sharnay Moultrie is an individual and a citizen and resident of Contra Costa County, California.

158. Plaintiff Moultrie is a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Moultrie took out a personal loan and obtained a credit card through Prosper.

159. Plaintiff Moultrie provided her PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Moultrie would not have provided her PII to Prosper had she had known it would be stored using inadequate data security and left vulnerable to a cyberattack.

160. Plaintiff Moultrie greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff Moultrie diligently protects her PII and stores any documents containing PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

161. At the time of the Data Breach, Prosper retained Plaintiff Moultrie's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Moultrie's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

162. On or about September 17, 2025, Prosper informed Plaintiff Moultrie that cybercriminals may have taken her sensitive PII in the Data Breach. Prosper has failed to provide Plaintiff Moultrie any update since that time that her PII was not, in fact, compromised.

163. Plaintiff Moultrie further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

164. Since the Data Breach, Plaintiff Moultrie has been the victim of attempted financial fraud. Specifically, unknown individuals attempted to make charges on two of Plaintiff Moultrie's credit cards. Plaintiff Moultrie had to close both credit cards and obtain new ones. Plaintiff Moultrie has also experienced an increase in spam text messages, emails, and phone calls since the Data Breach.

165. Plaintiff Moultrie has made reasonable efforts to mitigate the impact of the Data Breach, including reviewing financial account statements for any indications of actual or attempted identity theft or fraud, changing her credit cards after attempted fraud, freezing her loans, and deleting and being distracted by constant spam. Plaintiff Moultrie has spent many hours dealing with the Data Breach since learning about it, valuable time she otherwise would have spent on other activities.

166. Plaintiff Moultrie further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

167. Due to the Data Breach, Plaintiff Moultrie is at a present risk and will continue to be at risk of identity theft and fraud for years.

168. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

169. Plaintiff Moultrie has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

170. The Data Breach has also caused Plaintiff Moultrie to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

171. As a direct and traceable result of the Data Breach, Plaintiff Moultrie suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Childress's Experience

172. Plaintiff Joby Childress is an individual and a citizen and resident of Dalham County, Texas.

173. Plaintiff Childress was a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Childress took out personal loans with Prosper around 2007 or 2008 and again in 2012. Plaintiff Childress also applied for a third personal loan in 2021.

174. Plaintiff Childress provided his PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Childress would not have provided his PII to Prosper had he known it would be stored using inadequate data security and left vulnerable to a cyberattack.

175. Plaintiff Childress greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff Childress diligently protects his PII and stores any documents containing PII in a safe and secure location.

176. At the time of the Data Breach, Prosper retained Plaintiff Childress's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Childress's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

177. On or about September 17, 2025, Prosper informed Plaintiff Childress that his PII may have been taken by cybercriminals in the Data Breach. The website www.haveibeenpwned.com has also informed Plaintiff Childress that his PII was implicated in the Prosper Data Breach. According to this notification, the cybercriminals acquired files containing Plaintiff Childress's sensitive PII, including his government-issued IDs, date of birth, and credit status information.

178. Plaintiff Childress further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

179. Plaintiff Childress has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Childress has spent many hours dealing with the Data Breach since learning about it, valuable time he otherwise would have spent on other activities.

180. Plaintiff Childress further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

181. Due to the Data Breach, Plaintiff Childress is at a present risk and will continue to be at risk of identity theft and fraud for years.

182. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

183. Plaintiff Childress has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

184. The Data Breach has also caused Plaintiff Childress to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

185. As a direct and traceable result of the Data Breach, Plaintiff Childress suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Justiniano's Experience

186. Plaintiff Virginia Justiniano is an individual and a citizen and resident of Palm Beach County, Florida.

187. Plaintiff Justiniano applied for Prosper's financial services prior to the Data Breach. Specifically, Plaintiff Justiniano applied for a personal loan with Prosper around 2012 and again around 2018. Plaintiff Justiniano ultimately did not obtain any such financial services from Prosper.

188. Plaintiff Justiniano provided her PII to Prosper when she applied for financial services from Prosper. Plaintiff Justiniano would not have provided her PII to Prosper had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

189. Plaintiff Justiniano greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff Justiniano diligently protects her PII and stores any documents containing PII in a safe and secure location.

190. At the time of the Data Breach, Prosper retained Plaintiff Justiniano's PII in its databases and other systems. These databases and other systems were inadequately secured, which made it possible for Plaintiff Justiniano's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

191. On or about February 9, 2026, Prosper informed Plaintiff Justiniano that her PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals

acquired files containing Plaintiff Justiniano's sensitive PII, including her Social Security Number / National ID Number and date of birth.

192. Plaintiff Justiniano further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type. Further, Plaintiff Justiniano received an alert from an identity monitoring service that her confidential information had been found on the dark web following the Data Breach.

193. Since the Data Breach, Plaintiff Justiniano has been the victim of attempted financial fraud. On or around September 26, 2025, Plaintiff Justiniano discovered an unknown individual had withdrawn money from her bank account. While Plaintiff Justiniano's bank ultimately reversed the charge, she closed the account because of the attempted fraud. Plaintiff Justiniano has also experienced a significant increase in spam calls purporting to come from banks and financial institutions about loans they claim are in her name in the time since the Data Breach.

194. Plaintiff Justiniano has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Justiniano now monitors her financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

195. Plaintiff Justiniano further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

196. Due to the Data Breach, Plaintiff Justiniano is at a present risk and will continue to be at risk of identity theft and fraud for years.

197. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

198. Plaintiff Justiniano has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

199. The Data Breach has also caused Plaintiff Justiniano to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

200. As a direct and traceable result of the Data Breach, Plaintiff Justiniano suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Bell's Experiences

201. Plaintiff Elaine Melody Bell is an individual and a citizen and resident of Marion County, Indiana.

202. Plaintiff Bell is a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Bell made an investment with Prosper in or around early 2025. Through Prosper, Plaintiff Bell financed a loan for $1,000 over a three-year term.

203. Plaintiff Bell provided her PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Bell would not have provided her PII to Prosper had she known it would be stored using inadequate data security and left vulnerable to a cyberattack.

204. Plaintiff Bell greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff Bell diligently protects her PII and stores any documents containing PII in a safe and secure location. Plaintiff Bell also uses a secure password manager to store her credentials for her electronic accounts.

205. At the time of the Data Breach, Prosper retained Plaintiff Bell's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Bell's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

206. On or about December of 2025, Prosper informed Plaintiff Bell that her PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiff Bell's sensitive PII.

207. Plaintiff Bell further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

208. Since the Data Breach, Plaintiff has received numerous calls and emails claiming she has qualified for loans for which she did not apply, that accounts were opened in her name that she did not initiate, and that accounts she did not recognize were closed. Plaintiff Bell suspects that many of these emails were fraudulent phishing attempts, but she is not certain and is concerned about potential financial and identity fraud.

209. Plaintiff Bell has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Bell now monitors her financial and credit statements multiple times a week and has spent many hours dealing with the Data Breach since learning about it, valuable time she otherwise would have spent on other activities.

210. Plaintiff Bell further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

211. Due to the Data Breach, Plaintiff Bell is at a present risk and will continue to be at risk of identity theft and fraud for years.

212. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

213. Plaintiff Bell has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

214. The Data Breach has also caused Plaintiff Bell to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

215. As a direct and traceable result of the Data Breach, Plaintiff Bell suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Rivera's Experience

216. Plaintiff Ada Rivera is an individual and a citizen and resident of San Bernardino County, California.

217. Plaintiff Rivera was a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff Rivera took out a personal loan through Prosper.

218. Plaintiff Rivera provided her PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff Rivera would not have provided her PII to Prosper had she known it would be stored using inadequate data security and left vulnerable to a cyberattack.

219. Plaintiff Rivera greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff diligently protects her PII and stores any documents containing PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

220. At the time of the Data Breach, Prosper retained Plaintiff Rivera's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff Rivera's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

221. On or about September 17, 2025, Prosper informed Plaintiff Rivera that her PII may have been taken by cybercriminals in the Data Breach. Prosper has failed to provide Plaintiff Rivera any update since that time that her PII was not, in fact, compromised.

222. Plaintiff Rivera further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

223. Since the Data Breach, Plaintiff Rivera has been contacted twice by her bank with regard to attempted fraudulent charges and has had to change her debit card twice as a result. Plaintiff Rivera has also had an increase in spam phone calls and text messages since the Data Breach.

224. Plaintiff Rivera has made reasonable efforts to mitigate the impact of the Data Breach, including to reviewing her financial accounts statements for any indications of actual or attempted identity theft or fraud, communicating with her bank with regard to attempted fraudulent transactions, and signing up for a credit monitoring service. Plaintiff has spent many hours dealing with the Data Breach since learning about it, valuable time she otherwise would have spent on other activities.

225. Plaintiff Rivera further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

226. Due to the Data Breach, Plaintiff Rivera is at a present risk and will continue to be at risk of identity theft and fraud for years.

227. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

228. Plaintiff Rivera has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

229. The Data Breach has also caused Plaintiff Rivera to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

230. As a direct and traceable result of the Data Breach, Plaintiff Rivera suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff McPhee's Experience

231. Plaintiff Christopher McPhee is an individual and a citizen and resident of Alameda County, California.

232. Plaintiff McPhee is a customer of Prosper and received financial services from Prosper prior to the Data Breach. Specifically, Plaintiff McPhee applied and was approved for a consumer loan around 2018. He also obtained a credit card from Prosper around 2024.

233. Plaintiff McPhee provided his PII to Prosper as a condition of and in exchange for obtaining services from Prosper. Plaintiff McPhee would not have provided his PII to Prosper had he known it would be stored using inadequate data security and left vulnerable to a cyberattack.

234. Plaintiff McPhee greatly values her privacy and is very careful about sharing his sensitive PII. Plaintiff McPhee diligently protects his PII and stores any documents containing PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

235. At the time of the Data Breach, Prosper retained Plaintiff McPhee's PII in its databases and other systems. These databases and other systems were inadequately secured, which permitted Plaintiff McPhee's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

236. Prosper informed Plaintiff McPhee that his PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiffs' sensitive PII, including his Social Security number.

237. Plaintiff McPhee further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type. Further, Plaintiff McPhee has been alerted by his web browser and financial institution that his confidential information is on the dark web since the Data Breach.

238. Following the Data Breach, Plaintiff McPhee has been the victim of attempted financial fraud. Plaintiff McPhee has both received alerts that his payment cards were used to make suspicious charges and also discovered purchases he did not make in his payment card statements. As a result, he has twice needed to obtain a new payment card to prevent further financial fraud. Plaintiff McPhee also had to make changes to his automatic billing instructions tied to the compromised payment cards.

239. Plaintiff McPhee has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff McPhee now monitors his financial and credit statements multiple times a week and has spent many hours dealing with the Data Breach since learning about it, valuable time he otherwise would have spent on other activities.

240. Plaintiff McPhee further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

241. Due to the Data Breach, Plaintiff McPhee is at a present risk and will continue to be at risk of identity theft and fraud for years.

242. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

243. Plaintiff McPhee has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

244. The Data Breach has also caused Plaintiff McPhee to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

245. As a direct and traceable result of the Data Breach, Plaintiff McPhee suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff O'Neill's Experience

246. Plaintiff Heather O'Neill is an individual and a citizen and resident of Cumberland County, Pennsylvania.

247. To the best of her recollection, Plaintiff O'Neill has never applied for or obtained any financial services from Prosper.

248. Plaintiff O'Neill never directly provided her PII to Prosper and is unaware of how Prosper obtained her PII. Plaintiff O'Neill suspects Prosper purchased or otherwise obtained her PII from a third party.

249. Plaintiff O'Neill greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiffs diligently protect her PII and store any documents containing PII in a safe and secure location.

250. At the time of the Data Breach, Prosper retained Plaintiff O'Neill's PII in its databases and other systems. These databases and other systems were inadequately secured, which made it possible for Plaintiff O'Neill PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

251. Despite having never directly provided Prosper with her PII, on or about December 15, 2025, Prosper informed Plaintiff O'Neill that her PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiff O'Neill's sensitive PII, including her Social Security Number / National ID Number and date of birth.

252. Plaintiff O'Neill further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type. Further, since the Data Breach, Plaintiff O'Neill has received alerts on her credit report and in her web browser that her confidential information is on the dark web.

253. Plaintiff O'Neill has also noticed a significant increase in spam calls since the Data Breach.

254. Plaintiff O'Neill has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff O'Neill now monitors her financial and credit statements multiple times a week and has spent many hours dealing with the Data Breach since learning of it, valuable time she otherwise would have spent on other activities.

255. Plaintiff O'Neill further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

256. Due to the Data Breach, Plaintiff O'Neill is at a present risk and will continue to be at risk of identity theft and fraud for years.

257. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

258. Plaintiff O'Neill has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

259. The Data Breach has also caused Plaintiff O'Neill to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed her of key details about the Data Breach's occurrence, the information stolen, or how Prosper obtained Plaintiff O'Neill's PII in the first instance.

260. As a direct and traceable result of the Data Breach, Plaintiff O'Neill suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Palma's Experience

261. Plaintiff Felicity Palma is an individual and a citizen and resident of Providence County, Rhode Island.

262. Prior to the Data Breach, Plaintiff Palma applied for a loan and received an email from Prosper stating that she had applied for a WebBank loan through Prosper. To the best of her recollection, Plaintiff Palma did not directly provide her PII to Prosper. Plaintiff Palma did not obtain any financial services from Prosper.

263. Plaintiff Palma greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff Palma diligently protects her PII and stores any documents containing PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

264. At the time of the Data Breach, Prosper retained Plaintiff Palma's PII in its databases and other systems. These databases and other systems were inadequately secured, which made it possible for Plaintiff Palma's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

265. On or about December 9, 2025, Prosper informed Plaintiff Palma that her PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiff Palma's sensitive PII, including her Social Security Number/National ID Number and date of birth.

266. Plaintiff Palma further believes that her PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

267. Since the Data Breach, Plaintiff Palma has experienced an increase in spam text messages and calls. Plaintiff Palma also received a notification that her SSN is on the dark web.

268. Plaintiff Palma has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing financial account statements and identity monitoring services for any indications of actual or attempted identity theft or fraud. Plaintiff Palma has spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

269. Plaintiff Palma further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

270. Due to the Data Breach, Plaintiff Palma is at a present risk and will continue to be at risk of identity theft and fraud for years.

271. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

272. Plaintiff Palma has a continuing interest in ensuring that her PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

273. The Data Breach has also caused Plaintiff Palma to suffer fear, anxiety, and stress about her PII now being in the hands of cybercriminals, compounded by the fact that Prosper's still have not fully informed her of key details about the Data Breach's occurrence or the information stolen.

274. As a direct and traceable result of the Data Breach, Plaintiff Palma suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing her PII due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect her PII; (d) emotional distress because identity thieves now possess her sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

Plaintiff Fast's Experience

275. Plaintiff Hunter Fast is an individual and a citizen and resident of Dane County, Wisconsin.

276. Plaintiff Fast has never applied for or obtained any financial services from Prosper.

277. Plaintiff Fast never directly provided his PII to Prosper and is unaware of how Prosper obtained his PII. Plaintiff Fast suspects Prosper purchased or otherwise obtained his PII from a third party.

278. Plaintiff Fast greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff Fast diligently protects his PII and stores any documents containing PII in a safe and

secure location. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

279. At the time of the Data Breach, Prosper retained Plaintiff Fast's PII in its databases and other systems. These databases and other systems were inadequately secured, which made it possible for Plaintiff Fast's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

280. Despite having never directly provided Prosper with his PII, on or about December 11, 2025, Prosper informed Plaintiff Fast that his PII was taken by cybercriminals in the Data Breach. According to the Notice Email, the cybercriminals acquired files containing Plaintiff Fast's sensitive PII, including his Social Security Number/National ID Number and date of birth.

281. Plaintiff Fast further believes that his PII, and that of Class Members, was and will be sold and disseminated on illicit criminal networks, including through the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

282. Plaintiff Fast has made reasonable efforts to mitigate the impact of the Data Breach, including researching the Data Breach and reviewing credit monitoring service and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Fast now monitors his financial accounts and credit monitoring service frequently and has spent several hours dealing with the Data Breach since learning of it, valuable time he otherwise would have spent on other activities.

283. Plaintiff Fast further anticipates spending considerable resources, including time and money, on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

284. Due to the Data Breach, Plaintiff Fast is at a present risk and will continue to be at risk of identity theft and fraud for years.

285. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and misused, including through publication and dissemination on the dark web.

286. Plaintiff Fast has a continuing interest in ensuring that his PII, which remains in Prosper's possession, is protected and safeguarded from future breaches.

287. The Data Breach has also caused Plaintiff Fast to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Prosper still has not fully informed him of key details about the Data Breach's occurrence, the information stolen, or how Prosper obtained Plaintiff Fast's PII in the first instance.

288. As a direct and traceable result of the Data Breach, Plaintiff Fast suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy and deprivation of the right to exclude others from accessing his PII due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Prosper did not adequately protect his PII; (d) emotional distress because identity thieves now possess his sensitive PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Prosper obtained from Plaintiff and (g) other economic and non-economic harm.

IV. FACTUAL BACKGROUND

A. Prosper Collects and Maintains PII

289. Prosper is a financial services company offering a range of loan products and financial services to consumers and businesses.

290. Plaintiffs and Class Members are individuals whose data was compromised in the Data Breach. Plaintiffs and Class Members fall into two distinct categories: those who knowingly engaged with Prosper, and those who did not.

1. The Customer Subclass

291. The first category of Plaintiffs and Class Members are current and former customers of Defendants who applied for or received services from Defendants prior to the Data Breach, including Plaintiffs Petty, Blandino Soto, Childress, Huff, Rivera, Moultrie, Castillo, Yoder, McPhee, Bell, Justiniano, Palma, Wions, and Pappadakis (the "Customer Subclass"). As a condition of receiving financial services from Defendants, Defendants' customers, including Customer

Plaintiffs and Customer Subclass Members, were required to entrust Defendants with highly sensitive PII, including their names, Social Security numbers, and other sensitive data.

292. In exchange for receiving Customer Plaintiffs' and Customer Subclass Members' PII, Defendants promised to safeguard the sensitive, confidential data and use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

2. The No Relationship Subclass

293. The second category of Plaintiffs and Class Members are individuals who did not knowingly enter into a relationship with Prosper or provide Prosper with their PII but have been informed by Prosper or through public repositories of information exposed through data breaches that their sensitive, confidential PII was exposed in the Data Breach (the "No Relationship Subclass"). This includes named Plaintiffs MacDonald, O'Neill, Fast, and Cooper. The No Relationship Subclass Members have never knowingly transacted or interacted with Prosper, and many were not familiar with Prosper before they received notice of the Data Breach.

294. Beyond the PII Prosper collects from Customer Subclass Members who knowingly request and/or obtain financial services from it, Prosper has aggressively sought to obtain PII of non-customers through other means, which are often opaque. For example, buried deep within Prosper's annual filing with the Securities and Exchange Commission ("Form 10-K"), Prosper explains that it develops its risk assessment for loan applications in part on "a data archive from a consumer credit bureau."[9] Prosper also describes in its Form 10-K that it purchases existing loans from other lending institutions and thus acquires the PII of those borrowers without their knowledge.[10]

[9] Prosper Marketplace, Inc., Prosper Funding LLC, Annual Report (Form 10-K), at 9 (Mar. 26, 2025).

[10] *Id.* at 49.

295. Additionally, Prosper offers its personal loan services through offer-comparison sites, such as Intuit's Credit Karma.[11] Individuals interested in obtaining a personal loan who use an offer-comparison service to obtain offers for loan terms may have the personal information they provide as part of their request shared with Prosper, even if they never receive or pursue a loan offer from Prosper.

B. Prosper Knowingly Collected and/or Obtained and Maintained the PII of Class Members While Representing It Would Be Adequately Secured

296. The information Prosper held in its computer networks at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

297. At all relevant times, Prosper knew it was storing and using its networks to store and transmit valuable, sensitive PII belonging to millions of consumers, including Plaintiffs and Class Members, and that as a result, its systems would be attractive targets for cybercriminals.

298. Prosper also knew that any breach of its networks and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose PII was compromised, as well as intrusion into those individuals' highly private financial information.

299. Defendants' Privacy Notice,[12] published on its website and in effect when the Data Breach took place, promises and warrants as follows:

> **How Prosper Secures Your Information**
> Prosper uses significant safeguards, including physical, technical (electronic), and operational controls to protect your personal information, both during transmission and once received. . . . Once on our system, personal information can only be read or written through defined service access points, the use of which is password-protected. Data security is achieved through technical safeguards

[11] *See, e.g.*, *Handpick Your Loan*, Creditkarma, https://www.creditkarma.com/lp/pl-loantest?lpconfig=editorial&s=bing&adcampaign=Personal-Loans_revmar_bing-search_all-web_none_non-brand_all_ckpl&adgroup=ck-pl&msclkid=e80e4fb9b6e219a36895267d99e6f314, (last accessed Mar. 25, 2026); Post by mad_gasser, Reddit (r/personalfinance), *PROSPER offer through Credit Karma claims $17K loan at 0.16% $569 per month for 36 mo interest and fees total $4321* (2020), https://www.reddit.com/r/personalfinance/comments/j0binv/prosper_offer_through_credit_karma_claims_17k/ (on file with counsel).

[12] *Prosper Privacy Policy & Federal Privacy Notice*, Prosper Funding LLC, https://www.prosper.com/legal/privacy-policy (last visited Oct. 29, 2025).

> that include a combination of encryption, firewalls, intrusion prevention system, malware detection system, and data loss prevention systems. Prosper also conducts vulnerability scans of applications and systems regularly. Access to the system is tightly controlled and limited to only those who have a need to access information. Administrative safeguards such as a security awareness program, background checks, and internal information use policy ensure that only trained and trusted staff are permitted to access personal information. . . .
>
> **Secure Data Center**
> We store all sensitive financial information in state-of-the-art, highly secure data centers that are audited per AICPA SOC for Service Organizations. Physical access to the data centers is strictly controlled and we use the latest threat prevention technologies such as network and web application firewalls, VPN, antivirus, Web filtering and antispam technologies.
>
> **How does Prosper protect my personal information?**
> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.

300. Prosper made promises and representations to the public, including Plaintiffs and Class Members, that the PII in its possession would be kept safe and confidential, that the privacy of that information would be maintained, and that Prosper would delete any sensitive information after it was no longer required to maintain it.

301. Defendants derived economic benefits from collecting Plaintiffs' and Class Members' PII. Without the required submission and collection of PII, Defendants could not perform their financial services operations as efficiently and would not be able to generate as much revenue from Plaintiffs.

302. By obtaining, using, and benefiting from Plaintiffs' and Class Members' PII, Prosper assumed legal and equitable duties and knew or should have known that it was responsible for protecting that PII from unauthorized access and disclosure.

303. Prosper had and has a duty to adopt reasonable measures to keep Plaintiffs' and Class Members' PII confidential and protected from involuntary disclosure to third parties, and to audit,

monitor, and verify the integrity of its IT networks, and train employees with access to use adequate cybersecurity measures.

304. Prosper had and has obligations created by the FTC Act, 15 U.S.C. § 45, the Gramm–Leach–Bliley Act, 15 U.S.C. § 6801 ("GLBA"), common law, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and protected from unauthorized disclosure. Prosper failed to do so.

C. Prosper Agreed to and Represented It Would Adequately Secure the PII of the Customer Subclass

305. Prosper made promises and representations to its customers, including Customer Plaintiffs and Customer Subclass Members, that the PII collected from them as a condition of obtaining financial services from Prosper would be kept safe and confidential, that the privacy of that information would be maintained, and that Prosper would delete any sensitive information after it were no longer required to maintain it.

306. Customer Plaintiffs and Customer Subclass Members relied on these promises and representations from Prosper, a sophisticated financial institution, to implement reasonable practices to keep their sensitive PII confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete PII from Defendants' systems when no longer necessary for its legitimate business purposes.

307. But for Defendants' promises to keep Customer Plaintiffs' and Customer Subclass Members' PII secure and confidential, Customer Plaintiffs and Customer Subclass Members would not have sought services from or entrusted their PII to Defendants. Consumers in general demand security to safeguard their PII, especially when sensitive financial information is involved.

308. Based on the foregoing representations and warranties and to obtain financial services from Defendants, Customer Plaintiffs and Customer Subclass Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their promises and obligations to keep such information confidential and protected against unauthorized access.

D. Defendants Failed to Adequately Safeguard Plaintiffs' and Class Members' PII, Causing the Data Breach

309. On September 1, 2025, Prosper discovered unauthorized activity on its systems and began an investigation into the extent of the attack. Prosper's investigation determined that the attackers were able to exfiltrate data from "company databases that store customer and applicant data" between June and August 2025.[13]

310. On or about September 17, 2025, Prosper began sending Plaintiffs and other Data Breach victims notice ("Notice Letters") informing them their PII may have been compromised in the Data Breach. Prosper states that it began sending additional notices in December 2025.[14] Yet, many individuals did not receive notice until months later. Some individuals have not received a notice from Prosper but have been notified through public repositories that their information was exposed in the Prosper Data Breach.

311. The Notice Letters generally inform as follows, in part:

> At Prosper, our values are very important to us and we prioritize accountability and integrity in all our actions. As part of that commitment, today I need to share important news with you that has just become public, but I wanted you to hear it directly from me.
>
> We recently discovered unauthorized activity on our systems. . . . We have evidence that certain personal information, including Social Security Numbers, was obtained[.]

312. Omitted from the Notice Letter were the details of the date or root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been provided to all Plaintiffs and Class Members, who retain a vested interest in ensuring their PII is protected.

---

[13] *Cybersecurity Incident Customer FAQs*, Prosper, https://www.prosper.com/legal/incident-response (accessed Mar. 10, 2026).

[14] *Prosper Notice of Data Breach*, Prosper, https://www.prosper.com/blog/prosper-notice-of-data-breach (accessed Mar. 23, 2026).

313. Thus, Defendants' purported "disclosure" amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

314. For No Relationship Plaintiffs and No Relationship Subclass Members, Prosper's failure to identify how it came to possess their PII creates additional mitigation challenges, as they cannot accurately assess what accounts or sources of information might have been impacted by the Data Breach.

315. Plaintiffs and Class Members who received delayed notice or have not been notified by Prosper that their information was exposed in the Data Breach were and continue to be unable to take steps to mitigate further harms caused by the Data Breach.

316. One of the few details Defendants have publicly revealed is that the hackers were able to obtain information from Defendants' databases. These treasure troves of PII should have been protected by extraordinarily strict access and authentication controls, vigilant monitoring for suspicious activity, and alerting that would prompt rapid responses from Defendants' information security personnel. Thus, the scant details Defendants have provided suggest that Defendants allowed stunning security lapses to exist in their network environment, making a major data breach all but certain.

317. Prosper's failure to disclose any substantive information about the Data Breach makes it challenging to identify which precise industry standard security measures it failed to implement, but given the small amount of information Prosper has disclosed—that attackers were able to access and run queries on its internal databases[15]—it is apparent that its security procedures and practices failed to meet multiple industry standards. Prosper failed to use reasonable security practices and procedures appropriate to the nature of the sensitive PII it collected and maintained from Plaintiffs and Class Members, and, given Prosper's failure to publicly disclose details of how

[15] *See id.*

the Data Breach occurred, Court intervention is necessary to ascertain precisely in what ways Prosper's security was deficient.

318. These failures by Prosper allowed and caused cybercriminals to target and access Prosper's network and exfiltrate files containing Plaintiffs and Class Member's PII. For example, if Defendants had implemented industry-standard logging, monitoring, and alerting systems—basic technical safeguards that any PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate malicious activity in Prosper's network systems for the period it took to carry out the Data Breach, including the reconnaissance necessary to identify where Prosper stored PII, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Prosper's system without being caught.

319. Prosper would have recognized the malicious activities detailed above if it implemented basic monitoring and detection systems or heeded the alerts generated from such systems, which would have enabled Prosper to stop the Data Breach or at least greatly reduce its impact.

320. Prosper's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiffs' and Class Members' PII, meaning Prosper had no effective means in place to ensure that cyberattacks were detected and prevented.

E. Defendants Knew of the Risk of a Cyberattack Because Financial Institutions in Possession of PII are Particularly Susceptible

321. Defendants' negligence in failing to safeguard Plaintiffs' and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing such data.

322. Data thieves regularly target entities in the financial industry like Defendants due to the highly sensitive information such entities maintain. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

323. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

324. Cyber-attacks against financial institutions such as Defendants are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the Financial Sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[16]

325. In light of past high profile data breaches at companies across industries, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Progress Software (93.3 million records, May 2023), AT&T (51.2 million individuals, April 2024), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or, if acting as a reasonable financial institution, should have known that the PII it collected and maintained would be vulnerable to and targeted by cybercriminals.

326. As a financial institution in possession of consumers' PII, Prosper knew, or should have known, the importance of safeguarding the PII it obtained and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members due to a data breach. Nevertheless, Prosper failed to take adequate cybersecurity measures to prevent the Data Breach.

327. Despite the prevalence of public announcements of data breach and data security compromises, Prosper failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being wrongfully disclosed to cybercriminals.

328. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' PII compromised therein would be targeted by hackers and cybercriminals for use in variety of injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members'

[16] Contrast Security, *Cyber Bank Heists: Threats to the financial sector* at 5, https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last accessed Mar. 30, 2026).

PII can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

329. Prosper was, or should have been, fully aware of the significant volume of data on its systems, which included millions of individuals' sensitive PII, and, thus, the significant number of individuals who would be harmed by the exposure of that unencrypted data.

330. Plaintiffs and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

331. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and the like.

F. Defendants were Required, but Failed, to Comply with FTC Rules and Guidance

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

333. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses like Prosper. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17]

334. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

[17] Federal Trade Comm'n, *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Mar. 30, 2026).

someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

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

336. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures a business like Defendants must undertake to meet their data security obligations.

337. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect sensitive personal information, like PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

338. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[19]

339. Prosper failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

[18] *Id.*

[19] Pamela Jones Harbour, FTC Commissioner, Remarks Before FTC Exploring Privacy Roundtable (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

340. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

G. Defendant was Required, But Failed, to Comply With the GLBA

341. Under the GLBA, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

342. Defendants are financial institutions for purposes of the GLBA, because they are "significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities." 16 C.F.R. § 314.2(h).

343. "Nonpublic personal information" means "personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A)(i)–(iii).

344. The PII involved in the Data Breach constitutes "nonpublic personal information" for purposes of the GLBA.

345. Defendants collect "nonpublic personal information," as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) & 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendants were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801, *et seq*., and to numerous rules and regulations promulgated under the GLBA.

346. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (i) designating one or more employees to coordinate the information security program; (ii) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (iii) designing and implementing information safeguards to control the risks identified through risk

assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (iv) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (v) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 & 314.4. As alleged herein, Defendants violated the Safeguards Rule.

347. Defendants' conduct resulted in a variety of failures to follow GLBA mandated rules and regulations, many of which are also industry standards. Among such deficient practices, the Data Breach demonstrates that Defendants failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its information technology systems.

348. Had Defendants implemented data security protocols, the consequences of the Data Breach could have been avoided, or at least significantly reduced as the Data Breach could have been detected earlier, the amount of PII compromised could have been greatly reduced.

H. Defendants Failed to Comply with Industry Standards

349. What little information Prosper has made public about the Data Breach paints a stark picture of its information security controls. The one salient fact Prosper has disclosed—that attackers were able to access and run queries on its internal databases—indicates a cascading information security failure.[20] For the attackers to have been able to run such queries, Prosper necessarily had to violate numerous industry standards.

350. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

351. The Center for Internet Security's Critical Security Controls recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical

[20] *Prosper Notice of Data Breach*, Prosper, https://www.prosper.com/blog/prosper-notice-of-data-breach (accessed Mar. 23, 2026).

Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[21]

352. In addition, the NIST recommends certain practices to safeguard systems[22]:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

353. Further still, the Cybersecurity & Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT

[21] *See CIS Top 18 Critical Security Controls Solutions*, Rapid7, https://www.rapid7.com/solutions/compliance/critical-controls/ (last visited Oct. 29. 2025).

[22] Federal Trade Comm'n, Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf.

personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[23]

354. Defendants failed to implement industry standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' PII, resulting in the Data Breach.

I. Defendants Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their PII

355. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Prosper's duty owed to Plaintiffs and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure its computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' PII.

356. Prosper owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

357. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of PII in a timely manner and act upon data security warnings and alerts in a timely fashion.

[23] *Shields Up: Guidance for Organizations*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/shields-guidance-organizations (last visited Mar. 30, 2026).

358. Defendants owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

359. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

360. Defendants failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' PII from unauthorized disclosure. Defendants' actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

J. Plaintiffs and Class Members Suffered Common Injuries and Damages due to Defendants' Conduct

361. Defendants' failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' PII directly and proximately injured Plaintiffs and Class Members by the resulting disclosure of their PII in the Data Breach.

362. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

363. Plaintiffs and Class Members are also at a continued risk because their Private Information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect its customers' PII.

364. As a result of Defendants' ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their PII ending up in criminals' possession, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and they have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; (g) deprivation of their right to exclude others from accessing their PII; (h) loss of the benefit of their bargain with

Defendants; (i) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (j) the continued risk to their sensitive PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII Prosper collects and maintains.

1. Present and Ongoing Risk of Identity Theft

365. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

366. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[24] 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 "[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."[25]

367. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

368. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[26] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[27] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

---

[24] 17 C.F.R. § 248.201(b)(9) (2013).

[25] *Id.*

[26] Louis DeNicola, *What Is the Dark Web*, Experian Blog (May 12, 2021) https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last accessed Mar. 30, 2026).

[27] *Id.*

369. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal information like the PII at issue here.[28] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[29] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[30]

370. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Plaintiffs' and Class Members' PII.

371. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

372. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such

[28] *What is the Dark Web?*, Microsoft 365 Life Hacks, https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Mar. 30, 2026).
[29] *Id.;* Louis DeNicola, *What Is the Dark Web*, Experian Blog (May 12, 2021) https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Mar. 30, 2026).
[30] *What is the Dark Web?*, *supra* note 28.

as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

373. Identity thieves can also use an individual's personal data and PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, 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 issued in the victim's name.

374. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[31]

375. With "Fullz" packages, cybercriminals can cross-reference multiple sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

376. The development of "Fullz" packages means that the stolen PII from this Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII exfiltrated in

[31] "Fullz" is fraudster speak for data that includes the information of the victim, including the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz command $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last accessed Mar. 30, 2026).

the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

377. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

378. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

379. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen PII is being misused, and that such misuse is traceable to the Data Breach.

380. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[32]

381. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[33]

---

[32] Erika Harrell, *Victims of Identity Theft, 2018*, U.S. Department of Justice Office of Justice Programs Bureau of Justice Statistics (2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Mar. 30, 2026).

[33] *See 2019 Internet Crime Report Released*, Federal Bureau of Investigation, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Mar. 30, 2026).

382. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[34] Yet, Defendants failed to report to Plaintiffs and the Class in a timely manner that their PII was stolen.

383. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

384. In addition to out-of-pocket expenses that can exceed thousands of dollars, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

385. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

2. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

386. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

387. If Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face substantial costs and time to repair the damage to their good name and credit record.

[34] *Privacy: Lessons Learned about Data Breach Notification*, U.S. Government Accountability Office, GAO-07-657 (Apr. 2007), https://www.gao.gov/assets/gao-07-657.pdf.

388. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm.

389. Plaintiffs and Class Members have spent, and will spend, additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

390. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

391. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendants' conduct that caused the Data Breach.

3. Diminished Value of PII

392. Personal data like PII is a valuable property right.[36] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

[35] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last accessed Mar. 26, 2026).

[36] *See, e.g.*, John T. Soma, J. Zachary Coursin, and John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

393. An active and robust legitimate marketplace for personal information also exists. In 2025, the data brokering industry was worth roughly $300 billion.[37] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[38] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60 a year.[39]

394. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where it holds significant value for the threat actors.

395. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

4. Reasonable and Necessary Future Cost of Credit and Identify Theft Monitoring

396. To date, Defendants have done little to provide Plaintiffs and Class Members with relief for the damages they have suffered due to the Data Breach.

397. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that

[37] Data Broker Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031), Mordor Intelligence (Jan. 21, 2026), https://www.mordorintelligence.com/industry-reports/data-broker-market (last accessed Mar. 22, 2026)

[38] *See e.g.* Datacoup, https://datacoup.com/ (last accessed Mar. 30, 2026).

[39] Nielson Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (last accessed Mar. 30, 2026).

his or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

398. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[40] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

399. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

400. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendants' failure to safeguard their PII.

5. Deprivation of Property Right to Exclude Others from PII

401. Plaintiffs and the Class have a property interest in their PII.

402. This interest includes the right to exclude others from their property, and, thus, the right to exclude others from accessing their PII.

403. Plaintiffs and Class Members were deprived of their right to exclude others from accessing their PII when, because of the Data Breach, their PII was obtained by cybercriminals.

404. As discussed above, Plaintiffs and Class Members' loss of the right to exclude others from their PII is ongoing, due to the likelihood that their PII has or will end up on the dark web and will continuously be accessed, bought, or sold by nefarious actors in the future.

[40] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 26, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/ (last accessed Mar. 30, 2026).

6. Loss of Benefit of the Bargain

405. Furthermore, Defendants' poor data security deprived Customer Plaintiffs and Customer Subclass Members of the benefit of their bargain.

406. When agreeing to provide their PII, which was a condition precedent to obtaining services from Defendants, Customer Plaintiffs and Customer Subclass Members, as customers and consumers, understood and expected that they were, in part, paying for data security and the "significant safeguards" to protect their data that were promised by Prosper's privacy policy.

407. In fact, Defendants did not provide the expected data security. Accordingly, Customer Plaintiffs and Customer Subclass Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendants.

408. Had Customer Plaintiffs and Customer Subclass Members known about Defendants' inadequate security for their PII, they would have gone elsewhere for financial services and/or demanded better terms for their financial services or investments from Prosper.

K. Plaintiffs Lack an Adequate Remedy at Law

409. As described above, Plaintiffs suffer an actual and imminent threat of future harm that cannot be cured with monetary damages. Plaintiffs lack an adequate remedy at law for this future harm and require injunctive relief.

410. Plaintiffs seek equitable restitution under their UCL claim as an alternative to their damages claims. Plaintiffs' legal remedies are not adequate because they are not as certain as equitable restitution. For example, Plaintiffs are and will continue to be at imminent risk of identity fraud, such that they cannot reliably calculate the effect of Defendants' negligence and/or contractual breach so as to make them fully whole. Customer Plaintiffs also would not have purchased Defendants' products and services but for Defendants' misrepresentations about their cybersecurity practices, yet obtaining a full refund at law is less certain than at equity.

411. Proving damages for Plaintiffs' statutory claims is also more challenging and uncertain, requiring restitution to bridge the gap. For example, to obtain damages under the California Legal Remedies Act ("CLRA") and certain other state consumer protection statutes, Plaintiffs must demonstrate they satisfied the notice requirements, which Defendants may contest.

No such requirements exist to obtain restitution under the UCL. Additionally, the CLRA and other state consumer protection statutes prohibit more narrow categories of deceptive conduct, while the UCL broadly prohibits unfair and unlawful conduct. The same too for Plaintiffs' common law claims—the UCL was enacted specifically to create new claims and remedies not available at common law.

412. Finally, the remedies at law available to Plaintiffs are not equally prompt or otherwise efficient. The need to schedule a jury trial may result in delay. And a jury trial will take longer, and be more expensive, than a bench trial.

V. CLASS ACTION ALLEGATIONS

413. Plaintiffs bring this action on behalf of themselves and all other similarly situated persons pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), Plaintiffs seek to represent the following Class:

> All individuals in the United States whose PII was compromised in the Data Breach.

414. Plaintiffs also seek to represent the following Subclasses:

> **California Statutory Subclass:** All residents of California whose PII was compromised in the Data Breach.
>
> **Florida Statutory Subclass:** All residents of Florida whose PII was compromised in the Data Breach.
>
> **Colorado Statutory Subclass:** All residents of Colorado whose PII was compromised in the Data Breach.
>
> **New York Statutory Subclass:** All residents of New York whose PII was compromised in the Data Breach.
>
> **Customer Subclass:** All individuals in the United States who applied for a loan with Prosper, entered into a loan agreement with Prosper, obtained a credit card from Prosper, participated in Prosper's investment program, or otherwise knowingly obtained financial or credit services from Prosper and whose PII was compromised in the Data Breach.
>
> **No Relationship Subclass:** All individuals in the United States who did not knowingly obtain financial or credit services from Prosper and whose PII was compromised in the Data Breach.

415. Some Plaintiffs and Class Members, like Plaintiffs Petty, Rivera, Moultrie, Castillo, McPhee, O'Neill, Justiniano, and Pappadakis, are members of more than one subclass. For example, Plaintiff Castillo is a member of both the Customer Subclass and the California Statutory Subclass.

416. In addition or in the alternative, Plaintiffs will seek to represent additional state-based subclasses.

417. Excluded from the Class are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are attorneys for the Class or for Defendants. Also excluded are members of the judiciary to whom this case is assigned, their families, and members of their staff.

418. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division, or create and seek certification of additional classes, after having had an opportunity to conduct discovery.

419. Numerosity. The Class Members are so numerous that joinder of all of them is impracticable. While the precise number of Class Members at issue has not been determined, Plaintiffs believe the Data Breach affects millions of individuals.

420. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

421. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

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

b. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

d. Whether Defendants owed a duty to Class Members to safeguard their PII;

e. Whether Defendants breached their duty to Class Members to safeguard their PII;

f. Whether unauthorized hackers obtained Class Members' PII in the Data Breach;

g. Whether Defendants knew or should have known their data security systems and monitoring processes were deficient;

h. Whether Defendants' conduct was negligent;

i. Whether Defendants' conduct was in violation of the FTC Act and/or GLBA such that Defendants were negligent *per se*;

j. Whether Defendants' acts breached an implied contract formed with Plaintiffs and the Class Members;

k. Whether Defendants' acts violated the California Consumer Privacy Act;

l. Whether Defendants' acts violated California's Unfair Competition Law;

m. Whether Defendants' acts violated California's Customer Records Act;

n. Whether Defendants' acts violated the Colorado Consumer Protection Act;

o. Whether Defendants' acts violated the Florida Deceptive and Unfair Trade Practices Act;

p. Whether Defendants' acts violated the New York General Business Law;

q. Whether Defendants failed to provide notice of the Data Breach in a timely manner; and

r. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

422. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

423. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

424. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized

issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

425. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

426. Class certification is also appropriate because Defendants have acted or refused to act on grounds that apply generally to the Class as a whole, so that class certification, final injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

427. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

428. Issue Certification. In the alternative to class certification under Federal Rule of Civil Procedure 23(b)(2) and (b)(3), this case presents issues for which certification under Rule 23(c)(4) is appropriate. Such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CAUSES OF ACTION

CLAIM I: NEGLIGENCE/NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

429. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 428 as if fully set forth herein.

430. Defendants required Customer Plaintiffs and Class Members to submit sensitive, confidential PII to Defendants as a condition of receiving financial services from Defendants. Plaintiffs and Customer Subclass Members provided their PII to Defendants, including their names, Social Security numbers, and other sensitive data.

431. Defendants obtained sensitive and confidential PII of No Relationship Plaintiffs and Class Members without their knowledge. Defendants had full knowledge of the sensitivity of the PII which they obtained, and the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons.

432. Prosper owed a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the PII it collected.

433. Plaintiffs and Class Members were the foreseeable victims of any inadequate data safety and security practices by Defendants.

434. Plaintiffs and Class Members had no ability to protect their PII in Defendants' possession.

435. By collecting, transmitting, and storing Plaintiffs' and Class Members' PII Defendants owed Plaintiffs and Class Members a duty of care to use reasonable means to secure and safeguard their PII, to prevent the information's unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. Prosper's duties included the responsibility to implement processes by which it could detect and identify malicious activity or unauthorized access on its networks or servers.

436. Prosper owed a duty of care to Plaintiffs and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that controls for its networks, servers, and systems, and the personnel responsible for them, adequately protected Plaintiffs' and Class Members' PII.

437. Prosper's duty to use reasonable security measures arose because of the special relationship that existed between it and its customers, which is recognized by laws and regulations including the FTC Act, the GLBA, and the common law. Prosper was able to ensure its network

servers and systems were sufficiently protected against the foreseeable harm a data breach would cause Plaintiffs and Class Members, yet it failed to do so.

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

439. Pursuant to the FTC Act, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

440. Prosper breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices and procedures to safeguard Plaintiffs' and Class Members' PII, and by failing to ensure the PII in its systems was encrypted and timely delete when no longer needed.

441. Plaintiffs' and Class Members' injuries resulting from the Data Breach were directly and indirectly caused by Defendants' violations of the FTC Act.

442. Plaintiffs and Class Members are within the class of persons the FTC Act is intended to protect.

443. The type of harm that resulted from the Data Breach was the type of harm the FTC Act is intended to guard against.

444. Defendants' failure to comply with the FTC Act constitutes negligence *per se*.

445. The GLBA Safeguards Rule, as outlined *supra*, likewise establishes a standard of care that Defendants was obligated to follow, and is designed to safeguard financial services consumers from the type of harm inherent in data breaches and that was suffered here. Thus, Defendants' violation of the Safeguards Rule, as alleged above, constitutes negligence *per se*.

446. Prosper's duty to use reasonable care in protecting Plaintiffs' and Class Members' confidential PII in its possession arose not only because of the statutes and regulations described above, but also because Prosper is bound by industry standards to reasonably protect such PII.

447. Prosper breached its duties of care, and was grossly negligent and/or reckless, by acts of omission or commission, including by failing to use reasonable measures or even minimally

reasonable measures to protect the Plaintiffs' and Class Members' PII from unauthorized disclosure in this Data Breach.

448. The specific negligent acts and omissions committed by Defendants include the following:

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

b. Maintaining and/or transmitting Plaintiffs' and Class Members' PII in unencrypted and identifiable form;

c. Failing to implement data security measures, like adequate, phishing-resistant MFA for as many systems as possible, to safeguard against known techniques for initial unauthorized access to network servers and systems;

d. Failing to adequately train employees on proper cybersecurity protocols;

e. Failing to adequately monitor the security of its networks and systems;

f. Failure to periodically ensure its network system had plans in place to maintain reasonable data security safeguards;

g. Allowing unauthorized access to Plaintiffs' and Class Members' PII; and

h. Failing to adequately notify Plaintiffs and Class Members about the Data Breach so they could take appropriate steps to mitigate damages.

449. But for Defendants' wrongful and negligent breaches of their duties owed to Plaintiffs and Class Members, their PII would not have been compromised because the malicious activity would have been prevented, or at least, identified and stopped before criminal hackers had a chance to inventory Defendants' digital assets, stage them, and then exfiltrate them.

450. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs' and Class Members' PII would injure Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Defendants' industry.

451. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII would cause them one or more types of injuries.

452. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will suffer injuries, including (a) invasion of privacy; (b) lost or diminished value of their PII; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate

the actual consequences of the Data Breach, including lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their PII's disclosure to cybercriminals; (g) deprivation of their right to exclude others from accessing their PII; and (h) the continued and certainly increased risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect it.

453. Plaintiffs and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, as proven at trial. Plaintiffs and Class Members are also entitled to injunctive relief requiring Prosper to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate and lifetime credit monitoring to Plaintiffs and all Class Members.

CLAIM II: UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

454. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 428 as if fully set forth herein.

455. Plaintiffs plead this claim for unjust enrichment in the alternative to the breach of implied contract count below.

456. Prosper received a monetary benefit when it obtained Plaintiffs' and Class Members' PII, which Defendants used and depended on to operate their business. In exchange, Plaintiffs and Class Members should have had their PII protected with adequate data security.

457. Prosper knew that Plaintiffs and Class Members had conferred a benefit upon it, and accepted that benefit by retaining the PII and using it to generate revenue.

458. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided Defendants.

459. Prosper acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

460. Prosper enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of

providing a reasonable level of security that would have prevented the hacking incident, Prosper calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own pocket. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Prosper's decision to prioritize its own financial condition over the requisite security and the safety of customers' PII.

461. Under the circumstances, it would be unjust for Prosper to retain the benefits that Plaintiffs and Class Members conferred upon it.

462. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injuries and damages as set forth herein.

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

CLAIM III: BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs Petty, Blandino Soto, Childress, Huff, Rivera, Moultrie, Castillo, Yoder, McPhee, Bell, Justiniano, Palma, Wions, and Pappadakis. and the Customer Subclass)

464. Plaintiffs Petty, Blandino Soto, Childress, Huff, Rivera, Moultrie, Castillo, Yoder, McPhee, Bell, Justiniano, Palma, Wions, and Pappadakis ("Plaintiffs" for the purposes of this claim) re-allege incorporate by reference paragraphs 1 through 428 as if fully set forth herein. Plaintiffs bring this claim on behalf of the Customer Subclass.

465. Defendants required Plaintiffs and Customer Subclass Members to provide and entrust their PII to Defendants as a condition of and in exchange for receiving services from Defendants.

466. When Plaintiffs and Customer Subclass Members provided their PII to Defendants, they entered into implied contracts with Defendants, pursuant to which Defendants agreed to

safeguard and protect such PII and to timely and accurately notify Plaintiffs and Customer Subclass Members if and when their PII was breached and compromised.

467. Specifically, Plaintiffs and Customer Subclass Members entered into valid and enforceable implied contracts with Defendants when they agreed to provide their PII to Defendants, and Defendants agreed to reasonably protect it.

468. The implied contracts that Plaintiffs and Customer Subclass Members entered into with Prosper included Prosper's promises to protect PII it collected from Plaintiffs and Class Members, or created on its own, from unauthorized disclosures, including those contained in Prosper's Privacy Notice, set forth *supra* Section I, and manifested through Prosper's conduct in the mandatory collection of PII.

469. Plaintiffs and Customer Subclass Members provided their PII to Defendants in reliance on their promises.

470. Under the implied contracts, Defendants promised and were obligated to (a) provide services to Plaintiffs and Customer Subclass Members; and (b) protect Plaintiffs' and Customer Subclass Members' PII provided to obtain such services and/or created in connection therewith. In exchange, Plaintiffs and Customer Subclass Members agreed to provide Defendants with their PII.

471. Defendants promised and warranted to Plaintiffs and Customer Subclass Members to maintain the privacy and confidentiality of the PII collected from them, and to keep such information safeguarded against unauthorized access and disclosure.

472. Defendants' adequate protection of Plaintiffs' and Customer Subclass Members' PII was a material aspect of these implied contracts with Defendants.

473. Defendants solicited and invited Plaintiffs and Customer Subclass Members to provide their PII as part of Defendants' regular business practices. Plaintiffs and Customer Subclass Members accepted Defendants' offers and provided their PII to Defendants.

474. In entering into such implied contracts, Plaintiffs and Customer Subclass Members reasonably believed and expected that Defendants' data security practices complied with industry standards and relevant laws and regulations, including the FTC Act, the GLBA, and industry standards.

475. Plaintiffs and Customer Subclass Members, who contracted with Defendants for services including reasonable data protection and provided their PII to Defendants, reasonably believed and expected that Defendants would adequately employ adequate data security to protect that PII.

476. A meeting of the minds occurred when Plaintiffs and Customer Subclass Members agreed to, and did, provide their PII to Defendants and agreed Defendants would receive payment for, amongst other things, the protection of their PII.

477. Plaintiffs and Customer Subclass Members performed their obligations under the contracts when they provided their PII and/or payment to Defendants.

478. Prosper materially breached its contractual obligations to protect the PII it required Plaintiffs and Customer Subclass Members to provide when that PII was unauthorizedly disclosed in the Data Breach due to Prosper's inadequate data security measures and procedures.

479. Prosper materially breached its contractual obligations to deal in good faith with Plaintiffs and Customer Subclass Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify Plaintiffs and Customer Subclass Members of the Data Breach.

480. Prosper materially breached the terms of its implied contracts, including by failing to comply with industry standards or the standards of conduct embodied in statutes or regulations like Section 5 of the FTC Act and the GLBA, and by failing to otherwise protect Plaintiffs' and Customer Subclass Members' PII, as set forth *supra*.

481. The Data Breach was a reasonably foreseeable consequence of Defendants' breaches of these implied contracts with Plaintiffs and Customer Subclass Members.

482. Due to Defendants' failures to fulfill the data protections promised in these contracts, Plaintiffs and Customer Subclass Members did not receive the full benefit of their bargains with Defendants, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiffs and Customer Subclass Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid and provided their PII for, and that which they received.

483. Had Prosper disclosed that its data security procedures were inadequate or that it did not adhere to industry standards for cybersecurity, neither Plaintiffs, Customer Subclass Members, nor any reasonable person would have contracted with Prosper.

484. Plaintiffs and Customer Subclass Members would not have provided and entrusted their PII to Defendants in the absence of the implied contracts between them and Defendants. Defendants breached the implied contracts they made with Plaintiffs and Customer Subclass Members by failing to safeguard and protect their PII and by failing to provide timely or adequate notice that their PII was compromised in and due to the Data Breach.

485. As a direct and proximate result of Prosper's breach of its implied contracts with Plaintiffs and Customer Subclass Members and the attendant Data Breach, Plaintiffs and Customer Subclass Members have suffered injuries and damages as set forth herein and have been irreparably harmed.

486. Plaintiffs and Customer Subclass Members are entitled to damages, including compensatory, punitive, and/or nominal damages, to be proven at trial.

CLAIM IV: VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
Bus. & Prof. Code § 17200 *et seq.* ("UCL")
(On Behalf of Plaintiffs and the Class)

487. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 428 as if fully set forth herein.

488. Plaintiffs plead this claim for equitable relief, including restitution and injunctive relief, in the alternative to their claims for damages.

489. Prosper is a "person" under Cal. Bus. & Prof. Code § 17201.

490. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

491. Prosper's acts, omissions, and conduct, as alleged herein, constitute "business practices" within the meaning of the UCL.

492. Prosper's actions as alleged herein in this Consolidated Amended Class Action Complaint constitute an "unlawful" practice as encompassed by Cal. Bus. & Prof. Code §§ 17200 et seq. because its actions: (a) constituted negligence and unjust enrichment; (b) constituted breach

of implied contract ; (c) violated the California Consumer Privacy Act; (d) violated the California Customer Records Act; (e) violated California, New York, Colorado, and Florida consumer protection laws; and (f) violated federal law and regulations, including the FTC Act.

493. Prosper's actions as alleged in this Class Action Complaint also constitute an "unfair" practice as encompassed by Cal. Bus. & Prof. Code §§ 17200 *et seq*., because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious. The harm caused by Prosper's wrongful conduct outweighs any utility of such conduct and has caused—and will continue to cause—substantial injury to the Class, including Plaintiffs. There were ample reasonably available alternatives that would have furthered Prosper's legitimate business practices, including using industry-standard technologies to protect data (*e.g.*, multi-factor authorization, effective encryption and anonymization, compartmentalization of sensitive data, software patches, limiting how much data any user may access, and the purging of data no longer necessary for Prosper's services). Prosper also unreasonably delayed in notifying Plaintiffs and the Class Members regarding the unauthorized release and disclosure of their PII.

494. Prosper profited from their unfair conduct without incurring the costs associated with maintaining a system for the storage of PII with adequate data security.

495. Prosper's conduct also is deceptive in violation of the UCL. Prosper's fraudulent business acts and practices include:

a. Failing to adequately secure the personal information of Plaintiff and Class Members from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts about Plaintiff and Class Members in a manner highly offensive to a reasonable person;

c. Enabling the disclosure of personal and sensitive facts about Plaintiff and Class Members without their informed, voluntary, affirmative, and clear consent; and

d. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiffs' and Class Members' personal information.

496. Prosper's omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of Plaintiffs' and Class Members' personal information.

497. Prosper's unlawful, unfair, and fraudulent business practices described herein; including Prosper's security practices, marketing decisions, and privacy policies, were conceived, reviewed, approved or otherwise controlled from Prosper's headquarters in California.

498. The harm from Prosper's conduct was not reasonably avoidable by consumers. Plaintiffs and Customer Subclass Members were required to provide their PII to Prosper to receive financial services. Plaintiffs and No Relationship Subclass Members were unaware that Prosper had obtained their PII. In either case, Plaintiffs and Class Members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures.

499. There were reasonably available alternatives that would have furthered Prosper's business interests of electronically maintaining their customers' information while protecting PII.

500. A reasonable person would regard Prosper's derelict data security and the Data Breach as important, material facts that could and should have been disclosed.

501. As a direct and proximate result of Prosper's unlawful, unfair, and fraudulent conduct, Plaintiffs lost money or property because their sensitive personal information experienced a diminution of value; because they lost time to monitoring their financial accounts for fraudulent activity; because of the current and/or future costs of credit and identity theft monitoring services; and because Plaintiffs suffered damage to and a loss of their property interest and right to exclude others from their PII. Additionally, Plaintiffs and Customer Subclass Members did not receive their full benefit of the bargain, because, as a result of Prosper's inadequate security measures, they received financial services that were less valuable than what they paid for. Plaintiffs and Class Members also face ongoing and impending damages related to theft of their PII.

502. Prosper's wrongful practices constitute a continuing course of unfair competition because Prosper has failed to remedy the lax security practices or even fully notify all affected persons. Plaintiffs and the Class seek equitable relief pursuant to Cal. Bus. & Prof. Code § 17203 to end Prosper's wrongful practices and require Prosper to maintain adequate and reasonable security measures to protect the PII of Plaintiffs and the Class.

503. Further, if an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Prosper has still not provided adequate information on the cause and scope of the Data Breach. Plaintiff and Class Members lack an adequate remedy at law that will reasonably protect against the risk of a further breach.

504. Plaintiffs and the Class also seek an order requiring Prosper to make full restitution of all monies they received through their wrongful conduct, along with all other relief permitted under Cal. Bus. & Prof. Code §§ 17200 *et seq*.

505. At all relevant times, Prosper was willfully and knowingly engaged in the use of an unlawful, unfair, and deceptive practice.

CLAIM V: VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100, *et. seq*. ("CCPA")
(On Behalf of Plaintiffs Castillo, Moultrie, Rivera, and McPhee, and members of the California Statutory Subclass and Customer Subclass)

506. Plaintiffs Castillo, Moultrie, Rivera, and McPhee ("Plaintiffs" for the purposes of this claim) re-allege and incorporate by reference paragraphs 1 through 428 as if fully set forth herein. Plaintiffs bring this claim on behalf of members of the California Statutory Subclass and Customer Subclass.

507. Plaintiffs and the members of the California Statutory Subclass and Customer Subclass are consumers as that term is defined in Cal. Civ. Code § 1798.140(i).

508. Prosper is a business as that term is defined in Cal. Civ. Code § 1798.140(d). Prosper is organized or operated for the profit or financial benefit of its owners. Prosper collects consumers' personal information (including that of Plaintiffs and the California Statutory Subclass and Customer Subclass) or such information is collected on Prosper's behalf, and Prosper determines the purposes and means of the processing of consumers' personal information. Prosper does business in California and had annual revenue substantially in excess of $25 million dollars in the preceding calendar year.[41]

[41] *See* https://www.sec.gov/Archives/edgar/data/1416265/000141626525000006/prosper-20241231.htm

509. The information accessed during the Data Breach constitutes "personal information" as that term is defined in Cal. Civ. Code § 1798.140(v)(1) and 1798.81.5 and included Social Security Numbers.

510. Under the CCPA, Prosper had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information that it stored. Cal. Civ. Code § 1798.150(a)(1).

511. Prosper's failure to prevent the Data Breach by implementing and maintaining reasonable security procedures and practices constitutes a breach of its duty under the CCPA.

512. As a result of the Data Breach, the nonencrypted and nonredacted personal information of Plaintiffs and the California Statutory Subclass and Customer Subclass was subject to unauthorized access and exfiltration, theft, or disclosures.

513. Plaintiffs and the California Statutory Subclass and Customer Subclass seek injunctive relief in the form of an order enjoining Prosper from continuing to violate the CCPA pursuant to Cal. Civ. Code § 1798.150(a)(1)(B). Such injunctive relief is particularly important because Prosper continues to hold the PII of Plaintiffs and the California Statutory Subclass and Customer Subclass. Plaintiffs and the California Statutory Subclass and Customer Subclass have an interest in ensuring that their PII is reasonably protected.

514. Section 1798.150(b) of the CCPA requires plaintiffs to provide a defendant with 30 days' notice before seeking statutory damages under the CCPA. In October of 2025, Plaintiff Castillo sent Defendants a CCPA notification letter regarding this Data Breach on behalf of herself and putative California Class Members. Defendants have failed to respond to this letter or provide any cure. Plaintiffs and California Subclass Members therefore seek actual damages or statutory damages of $750 per consumer under section 1798.150(a)(1)(A).

CLAIM VI: VIOLATION OF CALIFORNIA'S CUSTOMER RECORDS ACT
Cal. Civ. Code § 1798.80 *et seq.* ("CCRA")
(On Behalf of Plaintiffs Castillo, Moultrie, Rivera, and McPhee and the California Statutory Subclass)

515. Plaintiffs Castillo, Moultrie, Rivera, and McPhee ("Plaintiffs" for the purposes of this claim) re-allege and incorporate by reference paragraphs 1 through 428 as if fully set forth herein. Plaintiffs bring this claim on behalf of the California Statutory Subclass.

516. The California legislature enacted the California Customer Records Act ("CCRA") to "ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5.

517. The CCRA defines personal information as follows: "'Personal information' means either of the following: (A) An individual's first name of 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.

518. The information involved in the Data Breach included name, Social Security Number/National ID Number, date of birth, bank account number, Prosper account number, other financial/credit application information, driver's license number, marriage or birth certificate, passport number, tax information, and payment card number.

519. The PII involved in the Data Breach was unencrypted. Plaintiff McPhee had his Social Security Number exposed in the Data Breach. Plaintiffs Castillo, Moultrie, and Rivera were informed that their PII, such as name, Social Security Number/National ID Number, bank account number, Prosper account number, driver's license number, passport number, tax information, and payment card number were potentially exposed in the Data Breach.

520. The CCRA defines owns, licenses, and maintains as follows: "[T]he terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term 'maintain' includes personal information that a business maintains but does not own or license.'" Cal. Civ. Code § 1798.81.5(a)(2). Prosper owns, licenses, and/or maintains the PII that was involved in the Data Breach.

521. As a direct and proximate result of Defendants' violation of Cal. Civ. Code § 1798.82(b) and (d), Plaintiffs Castillo, Moultrie, Rivera, McPhee, and California Statutory Subclass Members suffered damages, as described above. Plaintiffs and California Statutory Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

CLAIM VII: VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. §§ 501.201, *et seq*.

(On Behalf of Plaintiff Justiniano and Members of the Florida Statutory Subclass)

522. Plaintiff Justiniano ("Plaintiff" for the purposes of this claim) re-alleges and incorporates by reference paragraphs 1 through 428 as if fully set forth herein. Plaintiff brings this claim on behalf of members of the Florida Statutory Subclass.

523. Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

524. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Florida Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures after previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security

statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Florida Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Florida Subclass 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 Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

525. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and the Florida Subclass Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

526. Had Defendants disclosed to Plaintiff and Florida Subclass Members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Florida Subclass Members' PII as part of the services Defendants provided and for which Plaintiff and Florida Subclass Members paid without advising Plaintiff and Florida Subclass Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Florida Subclass Members' PII. Accordingly, Plaintiff and Florida Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

527. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary

damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; deprivation of their right to exclude others from accessing their PII; and an increased, imminent risk of fraud and identity theft.

528. Plaintiff and Florida Subclass Members seek all monetary and nonmonetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIM VIII: VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §§ 6-1-101, *et seq*.
(On Behalf of Plaintiff Pappadakis and Members of the Colorado Statutory Subclass)

529. Plaintiff Pappadakis ("Plaintiff" for the purposes of this claim) re-alleges and incorporates by reference paragraphs 1 through 428 as if fully set forth herein. Plaintiff brings this claim on behalf of members of the Colorado Statutory Subclass.

530. Defendants are "persons" as defined by Colo. Rev. Stat. § 6-1-102(6).

531. Defendants engaged in "sales" as defined by Colo. Rev. Stat. § 6-1- 102(10).

532. Plaintiff and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by Defendants or their successors in interest to actual consumers.

533. Defendants engaged in deceptive trade practices in the course of their business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Knowingly making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Defendants knew or should have known that they were another;

c. Advertising services with intent not to sell them as advertised; and

d. Failing to disclose material information concerning their services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

534. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Colorado Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures after previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Colorado Subclass Members' Personal Information; 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 Colorado Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

h. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Colorado Subclass Members' Personal Information; and

i. 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 Colorado Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

535. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and Colorado Subclass Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and Colorado Subclass

Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

536. Defendants intended to mislead Plaintiff and Colorado Subclass Members and induce them to rely on their misrepresentations and omissions. Defendants intended to mislead Plaintiff and Colorado Subclass Members and induce them to rely on their misrepresentations and omissions.

537. Had Defendants disclosed to Plaintiff and Colorado Subclass Members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Colorado Subclass Members' Personal Information as part of the services Defendants provided and for which Plaintiff and Colorado Subclass Members paid without advising Plaintiff and Colorado Subclass Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Colorado Subclass Members' PII. Accordingly, Plaintiff and Colorado Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

538. Defendants acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act and recklessly disregarded Plaintiff's and Colorado Subclass Members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiff's and Colorado Subclass Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

539. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Colorado Subclass Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

540. Defendants' deceptive trade practices significantly affect the public because Prosper's marketplace has over two million customers and has provided access to over $30 billion in total funding.[42]

541. Plaintiff and Colorado Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages (for Defendants' bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

CLAIM IX: VIOLATION OF NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, *et seq*.
(On Behalf of Plaintiff Petty and Members of the New York Statutory Subclass)

542. Plaintiff Petty ("Plaintiff" for the purposes of this claim) re-alleges and incorporates by reference paragraphs 1 through 428 as if fully set forth herein. Plaintiff brings this claim on behalf of members of the New York Statutory Subclass.

543. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New York Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and New York Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

[42] *About Us*, Prosper, https://www.prosper.com/about (accessed Mar. 26, 2026).

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and New York Subclass 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 New York Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

544. Plaintiff and New York Subclass Members were deceived in New York. They also transacted with Defendants in New York by using Defendants' products in New York.

545. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and New York Subclass Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

546. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law and recklessly disregarded Plaintiff's and New York Subclass Members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiff's and New York Subclass Members' PII sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

547. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including: loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; deprivation of their right to exclude others from accessing their PII; and an increased, imminent risk of fraud and identity theft.

548. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including all New Yorkers affected by the Data Breach. Defendants' above-described deceptive and unlawful practices and acts caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

549. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Petty, Blandino Soto, MacDonald, Childress, Huff, Rivera, Moultrie, Castillo, Yoder, McPhee, Bell, O'Neill, Justiniano, Fast, Palma, Wions, Cooper, and Pappadakis, individually and on behalf of all others similarly situated, pray for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class and Subclasses, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class and Subclasses;

B. Awarding Plaintiffs and the Class damages that include applicable compensatory, actual, exemplary, statutory, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

F. Awarding attorneys' fees and costs, as allowed by law,

G. Awarding pre- and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

I. Any and all such relief to which Plaintiffs and the Class are entitled.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: March 30, 2026

By: */s/ David M. Berger*
David M. Berger (SBN 277526)
GIBBS MURA LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
Tel: (510) 350-9700
Fax: (510) 350-9701
dmb@classlawgroup.com

James J. Pizzirusso (admitted *pro hac vice*)
HAUSFELD LLP
1200 17th Street, N.W.
Suite 600
Washington, DC 20036
Tel: (202) 540-7200
Fax: (202) 540-7201
jpizzirusso@hausfeld.com

Co-Lead Counsel for Plaintiffs