David S. Casey, Jr., SBN 060768
dcasey@cglaw.com
Gayle M. Blatt, SBN 122048
gmb@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
CASEY GERRY FRANCAVILLA BLATT LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Melissa R. Emert (pro hac vice forthcoming)
Gary S. Graifman (pro hac vice forthcoming)
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road-Suite 200
Montvale, NJ 07645
Telephone: 201-391-7000
Facsimile: 201-307-1086
memert@kgglaw.com
ggraifman@kgglaw.com

Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO / OAKLAND DIVISION

RYAN TAYLOR and SARAH EDGLEY, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

PROSPER FUNDING, LLC, and PROSPER MARKETPLACE, INC.,

Defendants.

Case No. 4:25-cv-9278

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Upon personal knowledge as to their own acts, and based upon their investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiffs Ryan Taylor and Sarah Edgley (together "Plaintiffs"), on behalf of themselves and all others similarly situated, alleges as follows:

SUMMARY OF THE ACTION

1. Plaintiffs bring this class action against Defendants Prosper Funding, LLC ("Prosper Funding") and Prosper Marketplace, Inc. **(**"Prosper Marketplace") (collectively, "Defendants") for their failure to adequately secure and safeguard the personally identifying information ("PII" or "Private Information") of Plaintiffs and millions of other individuals—consisting of both borrowers and investors—whose data was entrusted to Defendants. The compromised PII includes, without limitation, names, Social Security numbers, dates of birth, government identification numbers, addresses, income and employment data, and other sensitive personal and financial information.

2. Defendant Prosper Marketplace operates a peer-to-peer ("P2P") lending platform that matches consumers seeking personal loans or home equity loans ("borrowers") with individuals and institutions who fund those loans ("investors"). Borrowers submit applications and financial information through Prosper's online platform to obtain loans, while investors use the same platform to fund fractional interests in those loans in exchange for periodic payments of principal and interest.

3. Defendant Prosper Funding is a subsidiary of Defendant Prosper Marketplace. Prosper Funding facilitates the lending process available through the marketplace and manages relationships between investors and borrowers.

4. In order to apply for loans or to fund them, both borrowers and investors are required to provide Defendants with extensive personal and financial data. Borrowers must supply identifying, employment, and financial details to assess creditworthiness, while investors must provide Social Security numbers, tax information, and linked bank accounts to comply with federal tax-reporting and anti-money-laundering laws. Defendants collected, stored, and maintained this information in centralized databases under their exclusive control. Because Defendants held this PII in trust for their borrowers and investors, they owed an affirmative duty to implement and maintain

reasonable, industry-standard security measures to protect that information against unauthorized access, theft, and misuse.

5. Defendants represented to their users that they would use "physical, technical (electronic) and operational" safeguards to secure Plaintiffs' and Class Members' Private Information in their published privacy policy.[1] Defendants promise that their users' personal Private Information is "tightly controlled and protected" from any unauthorized access.[2]

6. Despite those assurances and Defendants' statutory and regulatory duties to protect consumer and investor PII, on or about September 1, 2025**,** Defendants discovered that unauthorized third parties had infiltrated Prosper's computer systems and exfiltrated sensitive borrower and investor information **i**n a massive data breach (the "Data Breach").

7. Although Defendants knew that borrowers' and investors' Private Information had been accessed and copied by cybercriminals, they failed to notify affected individuals until September 17, 2025, approximately two weeks after discovery of the intrusion. During that delay, the stolen data began appearing for sale on underground forums and dark-web marketplaces.

8. Defendants' failure to maintain the Private Information of Plaintiffs and Class Members through the necessary procedures and protocols resulted in their systems becoming vulnerable to attack.

9. Defendants were aware of the extraordinary sensitivity and value of the PII they maintained—data that includes immutable identifiers such as Social Security numbers and financial account information—yet failed to take appropriate measures to secure it.

10. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names and other personal information to open new financial accounts, incur credit charges, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have

[1] *Prosper Privacy Policy & Federal Privacy Notice*, PROSPER, https://www.prosper.com/legal/privacy-policy (last accessed Oct. 24, 2025).
[2] *Id.*

devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

11. Defendants knew or should have known that their systems were inadequately protected and that such a breach was a highly foreseeable risk given the nature of the data they collect and the rise of ransomware and credential-theft attacks targeting financial-technology companies.

12. The Data Breach was directly and proximately caused by Defendants' negligent maintenance, storage and protection of the data they obtained from Plaintiffs and Class Members. They failed to implement adequate and reliable security practices necessary to protect their network from a foreseeable and preventable cyberattack. Through this negligent conduct, Plaintiffs' and Class Members' sensitive personal information was compromised by cybercriminals.

13. Had Defendants implemented a robust security program consistent with industry standards and best practices, as they claim, they could have prevented the data breach and the resulting harm to millions of victims. Plaintiffs and Class Members are now at a significantly increased and imminent risk of fraud, identity theft, and other criminal acts, which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time and money to protect their Private Information from further misuse by cybercriminals.

14. Plaintiffs, on behalf of themselves and all others similarly situated, herein alleges claims for negligence, breach of implied contract, invasion of privacy under Article I, Section 1 of the California Constitution, and violation of the California Customer Records Act, California Consumer Privacy Act of 2018, and California's Unfair Competition Law. Plaintiffs on behalf of themselves and the Class, seeks: (i) actual damages, economic damages, statutory damages, and nominal damages; (ii) punitive damages; (iii) fees and costs of litigation; (iv) injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII in Defendants' custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and for Defendants to provide long-term identity theft protective services to Plaintiffs and Class Members; and (v) such other relief as the Court deems just and proper.

PARTIES

A. Plaintiffs

15. Plaintiff Ryan Taylor is a resident and citizen of West Hills, California. Plaintiff Taylor has been an investor with Prosper since approximately January 2021.

16. Plaintiff Sarah Edgley is a resident and citizen of Killeen, Texas. Plaintiff Edgley has been a borrower with Prosper since March 2025.

B. Defendants

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

18. Defendant Prosper Marketplace is a corporation organized under laws of Delaware, with its principal place of business located at 221 Main Street, 3rd Floor, San Francisco, California 94105.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one member of the putative Class, as defined below, is a citizen of a state other than that of Defendants, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

20. This Court has general personal jurisdiction over Defendants because they maintain their principal place of business in San Francisco, California, regularly conduct business in California, and have sufficient minimum contacts in California, such as to not offend traditional notions of fair play and substantial justice.

21. Venue in this District is proper under 28 U.S.C. § 1391 because Defendants reside in this District and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, including Defendants collecting or storing the PII of Plaintiffs and the putative Class Members.

22. Divisional Assignment: This action arises in San Francisco County, where Defendants are headquartered and where a substantial portion of the acts and omissions giving rise

to Plaintiffs' claims occurred. Pursuant to Civil Local Rule 3-2(d) of the United States District Court for the Northern District of California, all civil actions that arise in San Francisco County shall be assigned to the San Francisco or Oakland Division.

FACTUAL BACKGROUND

A. Defendants Collect, Store, and Maintain Personally Identifiable Information

23. Founded in 2005, Defendants Prosper Marketplace, Inc. and its subsidiary Prosper Funding, LLC operate one of the first and largest peer-to-peer ("P2P") lending platforms in the United States. Through the Prosper platform, borrowers can apply for and obtain personal loans, home-equity loans, and related credit products, while investors, both individuals and institutions, fund those loans in exchange for periodic payments of principal and interest.

24. Prosper facilitates and services these lending relationships by collecting and evaluating borrower applications, assessing credit risk, originating and servicing loans, and managing investor accounts and repayment distributions. In doing so, Defendants obtain, store, and maintain vast quantities of PII belonging to both borrowers and investors.

25. Borrowers are required to provide sensitive personal and financial data, including names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, income and employment information, and bank-account details. Investors must likewise provide identifying and financial information, such as names, addresses, Social Security or tax-identification numbers, and linked bank-account information, to verify their identities and comply with federal tax-reporting and anti-money-laundering laws. [3]

26. Plaintiffs and Class Members are and/or were customers of Defendants, either as borrowers or as investors, who entrusted Defendants with their highly confidential PII with the reasonable expectation that Defendants would safeguard it through the use of adequate and industry-standard security practices.

27. Prosper Funding represents to its customers that "[e]nsuring that Prosper is private and safe is our highest priority" and that users' information "is kept in a state-of-the-art data center.

[3] Prosper Privacy Policy & Federal Privacy Notice, *available at* https://www.prosper.com/about (last accessed October 24, 2025).

Physical access is strictly controlled and we use the latest in threat prevention technologies including the very best in firewall, VPN, antivirus, Web filtering and antispam technologies."[4] Prosper further assures customers that it follows a "rigid privacy policy" and "very strict guidelines to protect your privacy," emphasizing that "Prosper does not sell, rent, or share your personal information with third parties for their marketing purposes."[5]

28. Irrespective of these claims, Defendants failed to reasonably protect and safeguard their systems from foreseeable and preventable attack by cybercriminals. This wrongful conduct resulted in the exfiltration of Plaintiffs' and Class Members' sensitive Private Information causing significant and lasting harm.

B. The Data Breach Exposed Valuable PII

29. On September 1, 2025, Prosper Marketplace, Inc. and Prosper Funding LLC "identified that an unauthorized third party gained access to the Company's systems that contain proprietary and confidential information." Prosper further disclosed that it had "evidence that confidential, proprietary, and personal information, including Social Security numbers, was obtained, including through unauthorized queries made on Company databases that store customer and applicant data."[6]

30. According to Prosper's Form 8-K, the Company's investigation was ongoing as of September 17, 2025, when it reported the incident to the U.S. Securities and Exchange Commission, stating that the attack involved "unauthorized queries" of databases containing customer and applicant information.[7] While Prosper has not confirmed the total number of affected records, independent cybersecurity researchers have reported that the dataset exposed in the attack contained approximately 17.6 million unique email addresses and associated personally identifiable

[4] *Security and Privacy at Prosper*, Prosper Funding LLC, https://www.prosper.com/legal/security (last visited Oct. 28, 2025).
[5] *Id*.
[6] Prosper Funding LLC & Prosper Marketplace, Inc., Current Report (Form 8-K) Item 8.01 (Sept. 17, 2025), available at https://www.sec.gov/Archives/edgar/data/1542574/000141626525000038/prosper-20250901.htm [hereinafter "Prosper Form 8-K"].
[7] *Id*.

information.[8]

31. On September 17, 2025, Prosper publicly disclosed the incident and directed affected individuals to its incident-response resources for further information.[9] Prosper confirmed that it had notified law enforcement and was providing notice to affected individuals consistent with state data-breach requirements.

32. The compromised data, as described in Prosper's disclosure and in independent forensic analyses, included confidential, proprietary, and personal information such as names, addresses, dates of birth, and Social Security numbers, as well as other information provided during loan applications and investor onboarding.[10] The affected population included both borrowers and investors who submitted personal and financial data to Prosper's lending platform.

33. The exposed dataset reportedly included names, home addresses, dates of birth, Social Security numbers, and in some instances, credit-status indicators, employment details, and income information. According to third-party reporting, the compromised database contained information for both borrowers and investors, many of whom provided sensitive financial and tax data for identity verification under federal lending and anti-money-laundering requirements.[11]

34. Despite Defendants' duties and commitments to safeguard sensitive and private information, Defendants failed to follow industry-standard practices in securing Plaintiffs' and the Class Members' PII, as evidenced by the Data Breach.

35. The Data Breach notice failed to provide information about how the Data Breach occurred, the identities of the criminals responsible for the breach, and what steps have been taken

[8] Ionut Arghire, *Prosper Data Breach Impacts 17.6 Million Accounts*, SecurityWeek (Oct. 17, 2025), https://www.securityweek.com/prosper-data-breach-impacts-17-6-million-accounts/; *Have I Been Pwned: Prosper Data Breach Impacts 17.6 Million Accounts*, Have I Been Pwned (Oct. 16, 2025), https://haveibeenpwned.com/Breach/Prosper; Connor Jones, *Have I Been Pwned Logs 17.6 M Victims in Prosper Breach*, The Register (Oct. 17, 2025), https://www.theregister.com/2025/10/17/prosper_breach/.

[9] Prosper Form 8-K, supra note 1.

[10] *Id.*; see also Arghire, supra note 3 (reporting exposed dataset contained PII including names, birthdates, and Social Security numbers).

[11] *Id.; Over 17 Million Victims Reported in Huge Prosper Data Breach — Here's What We Know So Far*, TechRadar (Oct. 20, 2025), https://www.techradar.com/pro/security/over-17-million-victims-reported-in-huge-prosper-data-breach-heres-what-we-know-so-far.

to prevent further attacks.

36. Without this information, the victims' ability to protect themselves and prevent further harm from occurring is considerably diminished.

37. Based on the information provided by Defendants, the cyberattack was orchestrated to gain access to the sensitive Private Information of individuals, including that of the Plaintiffs and Class Members and that the cybercriminals successfully obtained this information from Defendants' network.

38. Upon information and belief, the Private Information of millions of individuals was accessed during the security incident.

39. The Data Breach occurred as a direct result of Defendants' failure to employ adequate safeguards to secure the sensitive information they were required to protect.

C. Defendants Had Ample Notice That They Were Likely Cyberattack Targets

40. At all relevant times, Defendants knew, or should have known, that the PII they were entrusted with was a target for malicious actors. Defendants knew this given the unique type and the significant volume of data on their networks, servers, and systems, comprising individuals detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the PII would harm.

41. As custodians of Plaintiffs' and Class Members' PII, Defendants knew or should have known the importance of protecting their PII, and of the foreseeable consequences and harms to such persons if any data breach occurred.

42. According to the Consumer Financial Protection Bureau, the number of data breach and identity theft complaints it received grew from 14,319 in 2020 to 32,469 in 2022.[12] It is well known among companies that PII such as social security numbers and financial information is valuable and frequently targeted by criminals.

[12] *See Compromised: Why experts say data breaches are on the rise,* NBC 6 SOUTH FLORIDA, https://www.nbcmiami.com/responds/compromised-why-experts-say-data-breaches-are-on-the-rise/3473306/ (last accessed June 5, 2025).

43. The Federal Trade Commission has warned consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[13]

44. In April 2020, ZDNet reported that "ransomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[14]

45. Criminals can commit all types of fraud, including: obtaining a driver's license or official identification card in the victim's name but the thief's picture, using the victim's name and SSN to obtain government benefits, to obtain lending or lines of credit, filing a fraudulent tax return using the victim's information. Identity thieves may obtain a job using the victim's social security number, rent a house, or give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[15]

46. Defendants' security obligations were especially important due to the substantial increase of cyberattacks and data breaches in recent years.

47. Defendants knew or should have known that as large corporations, they are prime targets of ransomware actors. Defendants also knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

D. Defendants Breached Their Duties to Plaintiffs and Class Members and Failed to Comply with Regulatory Requirements and Industry Practices.

48. Because Defendants were entrusted with PII at all times herein relevant, Defendants owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in

[13] *See* What to Know About Identity Theft, FEDERAL TRADE COMMISSION (Sept. 2024), https://consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed June 5, 2025).
[14] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed Sept. 1, 2025).
[15] *See* Warning Signs of Identity Theft, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed June 5, 2025).

handling, using, maintaining, storing, and safeguarding the PII in their care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. Defendants also owed a duty to safeguard PII because they were on notice that they were handling highly valuable data and knew there was a significant risk they would be targeted by cybercriminals. Furthermore, Defendants knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

49. Security standards commonly accepted among businesses like Defendants that store PII include, without limitation:

i. Maintaining a secure firewall configuration;

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

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

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII;

viii. Monitoring for server requests from VPNs; and

ix. Monitoring for server requests for Tor exit nodes.

50. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[16] and protection of PII which includes basic security standards applicable to all types of businesses.[17]

51. The FTC recommends that businesses:

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

[16] Start with Security: A Guide for Business, FTC (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[17] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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

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

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

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

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

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

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

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

52. As described further below, Defendants owed a duty to safeguard PII under the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") to ensure that all information they received, maintained, and stored was secure. This statute was enacted to protect Plaintiffs and the Class Members from the type of conduct in which Defendants engaged, and the resulting harms Defendants proximately caused Plaintiffs and the Class Members.

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

54. Defendants breached their duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII within their systems and networks, failing to monitor their systems and networks to promptly identify and thwart suspicious activity, allowing unmonitored and unrestricted access to unsecured PII, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Members' confidential and private information. Additionally, Defendants breached their duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendants also violated their duties under the FTC Act.

55. Defendants failed to prevent the Data Breach. Had Defendants properly maintained and adequately protected their systems, servers, and networks, the Data Breach would not have occurred.

56. Additionally, the law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of PII to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendants further breached their duties by failing to provide any notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendants actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members.

E. The Experiences of Plaintiffs

Plaintiff Ryan Taylor

57. Plaintiff Ryan Taylor is and has been an investor with Prosper Funding since approximately January 2021. As part of his investor application and onboarding process, he provided Prosper with sensitive personally identifying information, including his name, address, date of birth, and Social Security number, which was required to comply with federal identity-verification and tax-reporting regulations. Since completing that initial application, Plaintiff Taylor has continued to maintain his Prosper investor account and to fund loans through the platform.

58. Plaintiff Taylor entrusted Defendants with his private and financial data and relied on Prosper's representations that it employed robust "physical, technical, and operational safeguards" to protect his information. As an investor, he reasonably expected that Prosper would use industry-standard security measures, in accordance with federal law, to safeguard his PII and ensure that his financial identity and investments remained secure.

59. On or about September 17, 2025, Plaintiff Taylor received an email titled "Notice of Cybersecurity Incident" from Prosper, signed by Prosper CEO David Kimball. The notice informed him that Prosper had "recently discovered unauthorized activity" on its systems and that personal information, including Social Security numbers, had been obtained by unauthorized actors. The letter further stated that Prosper had "no evidence of unauthorized access to customer accounts or funds," but admitted that certain personal information had been exposed and offered free credit monitoring services. See Ex. A (copy of notice).

60. Plaintiff Taylor was shocked and angered to learn that his Social Security number and other personal identifiers were compromised, especially because he had not recently provided any new information to Prosper and assumed his data—submitted years earlier as part of his investor registration—was safely protected. He felt particularly violated as an investor, having trusted Prosper to maintain secure systems to safeguard investors as well as borrower data.

61. Upon learning of the Data Breach, Plaintiff Taylor spent numerous hours reviewing the notification, researching the incident online, contacting Prosper's customer-support line, and

monitoring his credit and financial accounts for signs of suspicious activity. He has also initiated credit monitoring and placed alerts with major credit bureaus to guard against identity theft.

62. As a proximate result of the Data Breach, Plaintiff Taylor will continue to devote significant time and effort to mitigating and monitoring the misuse of his personal information for the foreseeable future. This ongoing self-surveillance—necessary to detect potential fraud, unauthorized account openings, or tax-related misuse—represents a continuing loss of time and peace of mind that cannot be recovered.

63. Plaintiff Taylor has experienced substantial anger, frustration, and distress knowing that his highly sensitive information, including his Social Security number, has been stolen and is now likely in the hands of cybercriminals. The anxiety and uncertainty caused by this breach constitute a recognized and compensable injury under law.

64. Plaintiff Taylor suffered actual injuries, including diminution in the value of his PII, loss of privacy, and impairment of the confidentiality of his information, which constitutes a form of intangible property. His PII, entrusted to Defendants as part of his investor relationship, was compromised and rendered vulnerable through Defendants' failure to implement reasonable cybersecurity safeguards.

65. As a direct and proximate result of the breach, Plaintiff Taylor faces an imminent and substantial risk of identity theft, fraudulent account openings, and misuse of his financial data by unauthorized third parties. Because Social Security numbers and other immutable identifiers cannot be changed, the harm to Plaintiff Taylor is ongoing and permanent.

66. Plaintiff Taylor has a continuing and personal interest in ensuring that his PII, which remains in Defendants' possession, is adequately protected from future unauthorized access or exfiltration.

67. Defendants deprived Plaintiff Taylor of the earliest possible opportunity to mitigate harm by delaying notice of the breach until September 17, 2025, even though unauthorized access was detected weeks earlier. This delay increased the risk that his personal information could be disseminated or misused before he had any chance to protect himself.

Plaintiff Sarah Edgley

68. Plaintiff Sarah Edgley has been a borrower with Prosper Funding since approximately March 2025. To obtain her Prosper loan, she was required to provide detailed personally identifying and financial information, including her name, address, email, telephone number, date of birth, Social Security number, employment information, and banking details, as part of Prosper's online loan-application and verification process. She remained an active borrower with Prosper as of September 2025.

69. Plaintiff Edgley entrusted Defendants with her highly sensitive financial and personal data, relying on Prosper's repeated assurances that it employed "state-of-the-art, highly secure data centers" and robust firewalls to protect customer information. She reasonably believed that Defendants would comply with their legal and contractual duties to safeguard her PII against unauthorized access or disclosure.

70. On or about September 17, 2025, Plaintiff Edgley received an email from Prosper titled "Notice of Cybersecurity Incident," signed by CEO David Kimball. The notice informed her that Prosper had "recently discovered unauthorized activity" on its systems and that certain personal information, including Social Security Numbers, had been accessed by unknown actors. The letter further acknowledged that Prosper was offering complimentary credit monitoring after the breach. See Ex. B (copy of notice).

71. Plaintiff Edgley was deeply concerned and upset upon learning that her private financial information, provided in confidence solely for the purpose of obtaining a loan, had been compromised. She felt particularly betrayed because she had relied on Prosper's representations that customer information was "tightly controlled and protected." As a borrower, she believed Prosper's lending platform operated under banking-industry standards for encryption and data security.

72. After receiving the notice, Plaintiff Edgley spent numerous hours researching the breach, reading online coverage, contacting Prosper's response hotline, and monitoring her own financial and credit accounts. In the weeks that followed, she observed a significant uptick in spam emails, phishing messages, and telemarketing calls, which she had not experienced before the breach and which she reasonably attributes to the unauthorized dissemination of her PII.

73. As a proximate result of the Data Breach, Plaintiff Edgley must devote continuing time and effort to monitoring her accounts, placing fraud alerts, and protecting her identity. This ongoing vigilance represents a loss of time, productivity, and peace of mind that cannot be restored.

74. Plaintiff Edgley has experienced persistent anxiety, frustration, and anger knowing that her sensitive data, including her Social Security number, has been exposed to cybercriminals. The uncertainty surrounding how and when her information may be misused has caused real emotional distress that goes far beyond ordinary worry or inconvenience.

75. Plaintiff Edgley suffered tangible injury, including diminution in the value of her PII and loss of privacy in confidential financial data that she entrusted to Defendants. Because this information has likely been exfiltrated, copied, and disseminated, it has lost its inherent value as a secure identifier.

76. Plaintiff Edgley faces an ongoing risk of identity theft, credit fraud, and phishing schemes due to Defendants' failure to secure her personal information. Since Social Security numbers and dates of birth cannot be changed, she remains exposed to future harm indefinitely.

77. Plaintiff Edgley has a continuing interest in ensuring that her PII, still in Defendants' custody—is adequately protected from further compromise. She seeks injunctive relief to compel Defendants to adopt and maintain adequate cybersecurity practices.

78. Defendants deprived Plaintiff Edgley of the earliest opportunity to protect herself by delaying notice of the breach until September 17, 2025, even though Prosper detected unauthorized activity weeks earlier. This delay increased the risk that her PII would be disseminated and misused before she could act to mitigate the harm.

F. Plaintiffs and the Class Suffered Actual and Impending Injuries Resulting from the Data Breach

79. As a proximate result of Defendants' completely unreasonable security practices, identity thieves now possess the sensitive PII of Plaintiffs and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to Plaintiffs and the Class. On the dark web—an underground Internet black market—criminals openly buy and sell stolen PII to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank

accounts, social media accounts, and credit cards, file false insurance claims or tax returns, or rack up other kinds of expenses.[18] And, "[t]he damage to affected [persons] may never be undone."[19]

80. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[20] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[21]

81. As a consequence of the Data Breach, Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it

[18] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (Jun. 7, 2021), FORBES, https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=ca928c05650d.

[19] *Id.*

[20] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Oct. 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[21] *Id.*

impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

CLASS ACTION ALLEGATIONS

82. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and (b)(3), and where applicable, 23(c)(4), Plaintiffs seek certification of the following Nationwide Class and California Subclass (collectively, the "Class"):

> **Nationwide Class:** All persons in the United States who were impacted by the Prosper Data Breach, including all persons who were sent notice by Prosper that their Personal Information was compromised as a result of the Data Breach (and each person a "Class Member").
>
> **California Subclass:** All persons in the State of California who were impacted by the Prosper Data Breach, including all persons who were sent notice by Prosper that their Personal Information was compromised as a result of the Data Breach (and each person a "Class Member").

83. Excluded from the Class are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

84. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

85. *Numerosity Under Rule 23(a)(1)*. The Class is so numerous that the individual joinder of all members is impracticable, and the disposition of the claims of all members of the Class in a single action will provide substantial benefits to the parties and the Court. Upon information and belief, Plaintiffs estimate that the Class is comprised of millions of Class Members. The Class is sufficiently numerous to warrant certification.

86. *Commonality Under Rule 23(a)(2)*. Common legal and factual questions exist that predominate over any questions affecting only individual members of the Class. These common

questions, which do not vary among members of the Class and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendants knew or should have known that their computer systems and networks were vulnerable to unauthorized third-party access or a cyberattack;

b. Whether Defendants failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that their computer systems and networks were protected;

c. Whether Defendants failed to take available steps to prevent and stop the Data Breach from occurring;

d. Whether Defendants failed to comply with their own policies and applicable laws, regulations and industry standards relating to data security;

e. Whether Defendants owed a legal duty to Plaintiffs and Class Members to protect their PII;

f. Whether Defendants breached any duty to protect the PII of Plaintiffs and Class Members by failing to exercise due care in protecting their sensitive and private information;

g. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of the PII of Plaintiffs and Class Members.

h. Whether Defendants provided timely, accurate, and sufficient notice of the Data Breach to Plaintiffs and the Class Members;

i. Whether Plaintiffs and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

j. Whether Plaintiffs and Class Members are entitled to injunctive or equitable relief, including restitution.

87. *Typicality Under Rule 23(a)(3)*. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs had their PII compromised in the Data Breach. Defendants' uniformly unlawful course of conduct injured Plaintiffs and Class Members.

88. *Adequacy of Representation Under Rule 23(a)(4)*. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class.

Plaintiffs have retained counsel competent and experienced in complex litigation and consumer protection class action matters such as this action, and Plaintiffs and their counsel intend to vigorously prosecute this action for the Class's benefit and have the resources to do so. Plaintiffs and their counsel have no interests adverse to those of the other members of the Class.

89. *Predominance and Superiority*. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of each Class Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Even if each Class Member could afford individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands or more individual cases proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

90. As a result of the foregoing, class treatment under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3), and (c)(4) is appropriate.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

91. Plaintiffs incorporate the above allegations as if fully set forth herein.

92. Because Defendants were entrusted with such PII at all times herein relevant, they owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII in their care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect

and thwart attempts at unauthorized access to their networks and systems. This duty arose independently from any contract.

93. Defendants knew, or should have known, of the risks inherent in collecting and storing massive amounts of PII, including the importance of adequate data security and the high frequency of ransomware attacks and well-publicized data breaches. Defendants owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendants' failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that sensitive information. Indeed, on their websites, Defendants commit to data privacy, including safeguarding PII.

94. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII by failing to limit access to this information to unauthorized third parties and by not properly supervising both the way the PII was stored, used, and exchanged, and those in their employ responsible for such tasks.

95. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

96. Defendants also had a common law duty to prevent foreseeable harm to others. Defendants had full knowledge of the sensitivity and high value of the PII that they stored and the types of foreseeable harm and injury-in-fact that Plaintiffs and Class Members could and would suffer if that PII were wrongfully disclosed, leaked, accessed, or exfiltrated. Defendants' conduct created a foreseeable and unreasonable risk of harm to Plaintiffs and Class Members, who were the foreseeable victims of Defendants' inadequate data security practices.

97. Defendants violated their duty to implement and maintain reasonable security procedures and practices, including through their failure to adequately restrict access to their systems that held millions of individuals' PII or encrypt or anonymize such data. Defendants' duty included,

among other things, designing, maintaining, and testing their information security controls to ensure that PII in their possession was adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

98. Defendants' duty of care also arose pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), under which Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiffs and Class Members.

99. The FTC Act was enacted to protect Plaintiffs and the Class Members from the type of wrongful conduct in which Defendants engaged.

100. Defendants' violation of the FTC Act constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect the group to which Plaintiffs belongs and to prevent the types of harm that resulted from the Data Breach.

101. Defendants breached their duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII within their systems and networks, failing to monitor their systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII no longer necessary for its provision of services to their customers, allowing unmonitored and unrestricted access to unsecured PII, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Members' confidential and private information. Additionally, Defendants breached their duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendants also violated their duties under the FTC Act.

102. The law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of PII to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Defendants further breached its duties by failing to provide any notice of

the Data Breach to Plaintiffs and Class Members. In so doing, Defendants actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members. Timely disclosure was necessary so that Plaintiffs and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; and (vi) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

103. Defendants failed to adopt reasonable data security measures, in breach of the duties they owed to Plaintiffs and Class Members.

104. Plaintiffs and Class Members had no ability to protect their PII once it was in Defendants' possession and control. Defendants were in an exclusive position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

105. But for Defendants' breach of duty to adequately protect Class Members' PII, Class Members' PII would not have been stolen. As a result of Defendants' negligence, Plaintiffs and Class Members suffered and will continue to suffer the various types of damages alleged herein. There is a temporal and close causal connection between Defendants' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

106. As a direct and traceable result of Defendants' negligence, Plaintiffs and the Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiffs and the Class include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendants; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets;

(vi) unauthorized use of compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

107. Defendants' negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendants' care, and its failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

108. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

SECOND CAUSE OF ACTION
Injunctive/Declaratory Relief
(On Behalf of Plaintiffs and the Nationwide Class)

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

110. Defendants owe a duty of care to Plaintiffs and Class Members, which required Defendants to adequately monitor and safeguard Plaintiffs' and Class Members' PII.

111. Defendants and their officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII belonging to Plaintiffs and Class Members.

112. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore,

Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII, and the risk remains that further compromises of their private information will occur in the future.

113. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to adequately secure the PII of Plaintiffs and the Class within its care, custody, and control under the common law, and Section 5 of FTC Act;

b. Defendants breached their duty to Plaintiffs and the Class by allowing the Data Breach to occur;

c. Defendants' existing data monitoring measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII of Plaintiffs and the Class within Defendants' custody, care, and control; and

d. Defendants' ongoing breaches of said duties continue to cause harm to Plaintiffs and the Class.

114. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident occurs, Plaintiffs and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiffs and the Class for the serious risks of future harm.

115. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

116. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or

cybersecurity incident, thus preventing future injury to Plaintiffs and the Class and other persons whose PII would be further compromised.

THIRD CAUSE OF ACTION
Invasion of Privacy Under California's Constitution (Article 1, § 1)
(On Behalf of Plaintiff Taylor and the California Subclass)

117. Plaintiff, individually and on behalf of the California Subclass, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

118. Plaintiff and California Subclass Members have an interest in: (1) precluding the dissemination and/or misuse of their Private Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites for the provision of credit reporting services without the risk of their data being exfiltrated.

119. Plaintiff and California Subclass Members had a reasonable expectation that their communications, identity, and other data would remain confidential, and Defendants would keep their platforms secure.

120. By failing to secure Plaintiff's and California Subclass Members' personal data, Defendants intentionally invaded Plaintiff's and California Subclass Members' right to privacy under the California Constitution.

121. This invasion of privacy is serious in nature, scope, and impact because it relates to consumers' Private Information. Moreover, it constitutes an egregious breach of the societal norms underlying the right of privacy.

122. As a result of Defendants' actions, Plaintiff and California Subclass Members have suffered harm and injury, including but not limited to invasion of their privacy rights.

123. Plaintiff and California Subclass Members have been damaged as a direct and proximate result of Defendants' invasion of privacy and are entitled to just compensation, including monetary damages.

124. Plaintiff and California Subclass Members seek appropriate relief for this injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests.

125. Plaintiff and California Subclass Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and California Subclass Members in conscious disregard of their rights.

126. Such damages are needed to deter Defendants from engaging in such conduct in the future.

127. Plaintiff also seeks other such relief as the Court may deem just and proper.

FOURTH CAUSE OF ACTION
Violation of the California Customer Records Act
Cal. Civ. Code §§ 1798.80 *et seq.* ("CCRA")
(On Behalf of Plaintiff Taylor and the California Subclass)

128. Plaintiff, individually and on behalf of the California Subclass, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

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

130. Defendants are businesses that own, maintain, or license personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass Members.

131. Defendants violated Cal. Civ. Code § 1798.81.5 by failing to implement reasonable measures to protect California Subclass Members' PII.

132. Businesses that own or license computerized data that includes personal information are required to notify California residents when their PII has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other

requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

133. Defendants are businesses that own or license computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

134. Plaintiff's and California Subclass Members' PII includes personal information identified in Cal. Civ. Code § 1798.82(h) such as their names, birthdates and Social Security numbers, and is thereby covered by Cal. Civ. Code § 1798.82.

135. Plaintiff and the California Subclass Members are "customers" within the meaning of Cal. Civ. Code § 1798.80(c), as their personal information was provided to Defendants in the process of receiving Prosper's lending or credit card services.

136. The Data Breach constituted a breach of Defendants' security systems, networks, and servers.

137. Because Defendants reasonably believed that Plaintiff and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

138. Defendants unreasonably delayed informing Plaintiff and the California Subclass Members about the breach of security of their PII after they knew the breach had occurred.

139. Upon information and belief, no law enforcement agency instructed Defendants that notification to California Subclass Members would impede an investigation.

140. Thus, by failing to disclose the Data Breach in a timely and accurate manner, Defendants also violated Cal. Civ. Code § 1798.82.

141. Pursuant to Cal. Civ. Code § 1798.84, "[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable," "[a]ny customer injured by a violation of this title may institute a civil action to recover damages," and "[a]ny business that violates, proposed to violate, or has violated this title may be enjoined."

142. As a direct and proximate result of Defendants' violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members were (and continue to be) injured and suffered (and will continue to suffer) damages, as described above.

143. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including, but not limited to, actual damages, any applicable statutory damages, and equitable and injunctive relief.

FIFTH CAUSE OF ACTION
Violation of the California Consumer Privacy Act
Civ. Code § 1798.100 *et seq.* ("CCPA")
(On Behalf of Plaintiff Taylor and the California Subclass)

144. Plaintiff, individually and on behalf of the California Subclass, incorporate the above allegations as if fully set forth herein.

145. Section 1798.150(a)(1) of the CCPA provides, "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(1)(A)] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

146. Plaintiff is a consumer and California resident as defined by Civil Code section 1798.140(i).

147. Defendants are businesses as defined by Civil Code section 1798.140(d)(2) because they are "organized or operated for the profit or financial benefit of [their] shareholders or other owners," and "collect[] consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determine[] the purposes and means of the processing of consumers' personal information, that do[] business in the state of California."

148. Plaintiff and California Subclass Members' personal information, as defined by Civil Code section 1798.140(v)(1), was subject to unauthorized access and exfiltration, theft, or disclosure. The Data Breach described herein exposed, without limitation, names, Social Security numbers, and birth dates.

149. Defendants maintained Plaintiff's and California Subclass Members' PII in a form that allowed criminals to access it.

150. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Defendants failed to monitor their systems to identify suspicious activity and allowed unauthorized access to Plaintiff's and California Subclass Members' PII.

151. Consistent with Civil Code Section 1798.150(b), Plaintiff will provide written notice to Defendants identifying the CCPA provisions that Defendants violated.

152. On behalf of California Subclass Members, Plaintiff presently seeks actual pecuniary damages and injunctive relief in the form of an order enjoining Defendants from continuing to violate the CCPA. Unless and until Defendants are restrained by order of the Court, its wrongful conduct will continue to cause irreparable injury to Plaintiff and the California Subclass.

153. If Defendants fail to timely rectify or otherwise cure the CCPA violations described herein, individually and on behalf of the California Subclass, Plaintiff reserves their right to amend this Class Action Complaint to seek statutory damages and any other relief the Court deems proper as a result of Defendants' CCPA violations pursuant to Cal. Civ. Code § 1798.150(a).

SIXTH CAUSE OF ACTION
Violation of the Unfair Competition Law
Bus. & Prof. Code § 17200 et seq. ("UCL")
(On Behalf of Plaintiffs and the Nationwide Class, or in the Alternative, the California Subclass)

154. Plaintiffs incorporate the above allegations as if fully set forth herein.

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

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

157. Defendants' actions as alleged herein in this Class Action Complaint constitute an "unlawful" practice as encompassed by Cal. Bus. & Prof. Code §§ 17200 *et seq.* because Defendants' actions: (a) violated the California Consumer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, (b)

violated the CCPA, Cal. Civ. Code §§ 1798.100 *et seq.*, (c) constituted negligence; and (d) violated federal law and regulations, including the FTC Act and HIPAA.

158. Defendants' 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 Defendants' 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 Defendants' legitimate business practices, including using industry-standard technologies to protect data (e.g., two-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 Defendants' services). Defendants also unreasonably delayed in notifying Plaintiffs and the Class Members regarding the unauthorized release and disclosure of their PII. Additionally, Defendants' conduct was "unfair" because it violated the legislatively declared policies reflected by California's strong data-breach and online-privacy laws, including the California Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, the CCPA, Cal. Civ. Code §§ 1798.100, *et seq.*, and the California constitutional right to privacy, Cal. Const. Art. 1, § 1.

159. Defendants' conduct also is deceptive in violation of the UCL. Defendants' fraudulent business acts and practices include:

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

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

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

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

160. Defendants' 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 the Class's personal information.

161. The harm from Defendants' conduct was not reasonably avoidable by consumers. Plaintiffs and Class Members were required to provide their PII to Prosper to receive lending or credit card services, which without their consent or knowledge, was in turn provided to Defendants. 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.

162. There were reasonably available alternatives that would have furthered Defendants' business interests of electronically transferring their customers' information while protecting PII.

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

164. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent conduct, Plaintiffs lost money or property because their sensitive personal information experienced a diminution of value and because they devoted additional time to monitoring their financial accounts for fraudulent activity. Plaintiffs face ongoing and impending damages related to theft of their PII.

165. Defendants' wrongful practices constitute a continuing course of unfair competition because, on information and belief, Defendants have failed to remedy the lax security practices or even fully notify all affected Class Members. Plaintiffs and the Class seek equitable relief pursuant to Cal. Bus. & Prof. Code § 17203 to end Defendants' wrongful practices and require Defendants to maintain adequate and reasonable security measures to protect the PII of Plaintiffs and the Class.

166. Plaintiffs and Class Members lack an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages, ongoing identity theft and fraud, as well as long term incalculable risk associated with medical fraud.

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

168. Plaintiffs and the Class Members also seek an order requiring Defendants 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.*

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves the Class and the California Subclass set forth herein, respectfully request the following relief:

A. Certifying this action as a class action under Fed. R. Civ. P. 23 and appointing Plaintiffs and their counsel to represent the Class and California Subclass;

B. Entering judgment for Plaintiffs and the Class, and the California Subclass;

C. Granting permanent and appropriate injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendants to adequately safeguard the PII of Plaintiffs, the Class, and the California Subclass by implementing improved security controls;

D. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

E. Award Plaintiffs, the Class, and the California Subclass statutory or punitive damages as allowed by law in an amount to be determined at trial;

F. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of Defendants' unlawful acts, omissions, and practices;

G. Awarding to Plaintiffs, the Class, and the California Subclass the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

I. Granting such further and other relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all claims so triable.

Dated: October 28, 2025

CASEY GERRY FRANCAVILLA BLATT LLP

/s/ David S. Casey, Jr.
David S. Casey, Jr., SBN 060768
Gayle M. Blatt, SBN 122048
P. Camille Guerra, SBN 326546
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
dcasey@cglaw.com
gmb@cglaw.com
camille@cglaw.com

Melissa R. Emert (*pro hac vice forthcoming*)
Gary S. Graifman (*pro hac vice forthcoming*)
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road
Suite 200
Montvale, NJ 07645
Telephone: (201) 391-7000
E-mail: memert@kgglaw.com
ggraifman@kgglaw.com

Counsel for Plaintiffs and the Proposed Class