

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Catherine Ybarra (SBN 283360)
Tyler J. Bean (*pro hac vice* to be filed)
Neil Williams (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
700 S Flower St, Ste 1000,
Los Angeles, CA 90017
Tel: (646) 357-1732
E: cybarra@sirillp.com
E: tbean@sirillp.com
E: nwilliams@sirillp.com

Attorneys for Plaintiff and the Proposed Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

<p>BILLY YODER, on behalf of himself and all others similarly situated,</p> <p style="text-align: center;">Plaintiff,</p> <p>v.</p> <p>PROSPER FUNDING LLC,</p> <p style="text-align: center;">Defendant.</p>	<p>Case No.</p> <p>CLASS ACTION COMPLAINT</p> <p>JURY TRIAL DEMANDED</p>
---	--

CLASS ACTION COMPLAINT

Plaintiff Billy Yoder (“Plaintiff”), individually and on behalf of all similarly situated persons, allege the following against Prosper Funding LLC (“Prosper” or “Defendant”) based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff’s counsel and review of public documents as to all other matters:

I. INTRODUCTION

1
2 1. Plaintiff brings this class action against Prosper for its failure to properly secure and
3 safeguard Plaintiff’s and other similarly situated Prosper customers’ names and contact
4 information, dates of birth, Social Security numbers, and account information tied to applications
5 (the “Private Information”) from hackers.
6

7 2. Prosper, based in San Francisco, is a peer-to-peer lending company that serves
8 helped over 1.7 million people nationwide access more than \$27 billion in loans.

9 3. On or about September 17, 2025, Prosper filed official notice of a hacking incident
10 with the United States Securities and Exchange Commission.

11 4. On or around the same time, Prosper also sent out emailed data breach letters (the
12 “Notice”) to individuals whose information was compromised as a result of the hacking incident.
13

14 5. Based on the Notice, Prosper detected unusual activity on some of its computer
15 systems on September 1, 2025. In response, the company conducted an investigation which
16 revealed that an unauthorized party had access to certain company files (the “Data Breach”).

17 6. Plaintiff and “Class Members” (defined below) were, and continue to be, at
18 significant risk of identity theft and various other forms of personal, social, and financial harm. The
19 risk will remain for their respective lifetimes.

20 7. The Private Information compromised in the Data Breach included highly sensitive
21 data that represents a gold mine for data thieves, including but not limited to, financial account
22 information and Social Security numbers that Prosper collected and maintained.
23

24 8. Armed with the Private Information accessed in the Data Breach, data thieves can
25 commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members’
26 names, taking out loans in Class Members’ names, using Class Members’ information to obtain
27
28

1 government benefits, filing fraudulent tax returns using Class Members' information, and giving
2 false information to police during an arrest.

3 9. There has been no assurance offered by Prosper that all personal data or copies of
4 data have been recovered or destroyed, or that Defendant has adequately enhanced its data security
5 practices sufficient to avoid a similar breach of its network in the future.

6
7 10. Therefore, Plaintiff and Class Members have suffered and are at an imminent,
8 immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from
9 identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of
10 their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach,
11 and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12
13 11. Plaintiff brings this class action lawsuit to address Prosper's inadequate
14 safeguarding of Class Members' Private Information that it collected and maintained.

15
16 12. The potential for improper disclosure and theft of Plaintiff's and Class Members'
17 Private Information was a known risk to Prosper, and thus Prosper was on notice that failing to take
18 necessary steps to secure the Private Information left it vulnerable to an attack.

19
20 13. Upon information and belief, Prosper and its employees failed to properly
21 implement security practices with regard to the computer network and systems that housed the
22 Private Information.

23
24 14. Plaintiff's and Class Members' identities are now at risk because of Prosper's
25 negligent conduct as the Private Information that Prosper collected and maintained is now in the
26 hands of data thieves and other unauthorized third parties.

27
28 15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated
individuals whose Private Information was accessed and/or compromised during the Data Breach.

1 IV. FACTUAL ALLEGATIONS

2 *A. Prosper's Business and Collection of Plaintiff's and Class Members' Private*
3 *Information*

4 22. Prosper is a peer-to-peer lending company. Founded in 2005, Prosper is one of the
5 first peer-to-peer lending companies in the United States, serving customers across the country.
6 Prosper is a wholly owned subsidiary of Prosper Marketplace, Inc. Prosper employs more than 520
7 people and generates approximately \$137.7 million in annual revenue.

8 23. As a condition of receiving lending services, Prosper requires that its customers
9 entrust it with highly sensitive personal information. In the ordinary course of receiving service
10 from Prosper, Plaintiff and Class Members were required to provide their Private Information to
11 Defendant.

12 24. Prosper uses this information, *inter alia*, to process transactions, supporting internal
13 business operations, and marketing.

14 25. In its privacy policy, Prosper promises its customers that it will not share this Private
15 Information with third parties:

16 Prosper equips all servers with a Secure Socket Layer (SSL) certificate to ensure
17 that when you connect to our websites, you can tell that you are on a Prosper website
18 and that all data entered into the websites are transmitted to us in a secure encrypted
19 channel. Once on our system, personal information can only be read or written
20 through defined service access points, the use of which is password-protected. Data
21 security is achieved through technical safeguards that include a combination of
22 encryption, firewalls, intrusion prevention system, malware detection system, and
23 data loss prevention systems. Prosper also conducts vulnerability scans of
24 applications and systems regularly.

1 Access to the system is tightly controlled and limited to only those who have a need
2 to access information. Administrative safeguards such as a security awareness
3 program, background checks, and internal information use policy ensure that only
4 trained and trusted staff are permitted to access personal information.¹
5

6 26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class
7 Members' Private Information, Prosper assumed legal and equitable duties and knew or should
8 have known that it was responsible for protecting Plaintiff's and Class Members' Private
9 Information from unauthorized disclosure and exfiltration.

10
11 ***B. The Data Breach and Prosper's Inadequate Notice to Plaintiff and Class Members***

12 27. According to Defendant's Notice, it learned of unauthorized access to its computer
13 systems on September 1, 2025, with such unauthorized access having taken place on or around the
14 same day.

15
16 28. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of
17 highly sensitive Private Information, including full names and contact information, dates of birth
18 and Social Security numbers, and address details and account information tied to applications of
19 potentially thousands of individuals.

20 29. On or about September 17, 2025, roughly two weeks after Prosper learned that the
21 Class's Private Information was first accessed by cybercriminals, Prosper began to notify customers
22 that its investigation determined that their Private Information was impacted.
23
24
25
26

27
28

¹ <https://www.prosper.com/legal/privacy-policy> (last visited on Sept. 18, 2025).

1 30. Prosper emailed Data Breach Notification Letters to Plaintiff and Class Members,
2 alerting them that their highly sensitive Private Information had been exposed in a “Cybersecurity
3 Incident.”

4 31. Omitted from the Notice are crucial details like the root cause of the Data Breach,
5 the vulnerabilities exploited, the unauthorized actor responsible for the Data Breach, and the
6 remedial measures undertaken to ensure such a breach does not occur again. To date, these critical
7 facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested
8 interest in ensuring that their Private Information is protected.

9 32. Thus, Prosper’s purported disclosure amounts to no real disclosure at all, as it fails
10 to inform Plaintiff and Class Members of the Data Breach’s critical facts with any degree of
11 specificity. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms
12 resulting from the Data Breach was and is severely diminished.

13 33. In addition, the Notice offers no substantive steps to help victims like Plaintiff and
14 Class Members to protect themselves other than providing limited credit monitoring – an offer that
15 is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiff
16 and Class Members now face as a result of the Data Breach.

17 34. Prosper had obligations created by contract, industry standards, common law, and
18 representations made to Plaintiff and Class Members to keep Plaintiff’s and Class Members’
19 Private Information confidential and to protect it from unauthorized access and disclosure.

20 35. Plaintiff and Class Members provided their Private Information to Prosper with the
21 reasonable expectation and mutual understanding that Prosper would comply with its obligations
22 to keep such information confidential and secure from unauthorized access and to provide timely
23 notice of any security breaches.
24
25
26
27
28

1 36. Prosper’s data security obligations were particularly important given the substantial
2 increase in cyberattacks in recent years.

3 37. Prosper knew or should have known that its electronic records would be targeted by
4 cybercriminals.

5
6 ***C. Prosper Knew or Should Have Known of the Risk of a Cyber Attack Because***
7 ***Businesses in Possession of Private Information are Particularly Susceptible.***

8 38. Prosper’s negligence, including its gross negligence, in failing to safeguard
9 Plaintiff’s and Class Members’ Private Information is particularly stark, considering the highly
10 public increase of cybercrime similar to the hacking incident that resulted in the Data Breach.

11
12 39. Data thieves regularly target entities like Prosper due to the highly sensitive
13 information they maintain. Prosper knew and understood that Plaintiff’s and Class Members’
14 Private Information is valuable and highly sought after by criminal parties who seek to illegally
15 monetize it through unauthorized access.

16
17 40. According to the Identity Theft Resource Center’s 2023 Data Breach Report, the
18 overall number of publicly reported data compromises in 2023 increased more than 72-percent over
19 the previous high-water mark and 78-percent over 2022.²

20
21 41. Despite the prevalence of public announcements of data breach and data security
22 compromises, Prosper failed to take appropriate steps to protect Plaintiff’s and Class Members’
23 Private Information from being compromised in this Data Breach.

24
25
26
27 ² 2023 Annual Data Breach Report, IDENTITY THEFT RESOURCE CENTER, (Jan. 2024), available online at:
28 https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last visited on Sept. 18, 2025).

1 42. As a national service provider in possession of millions of customers' Private
2 Information, Prosper knew, or should have known, the importance of safeguarding the Private
3 Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences
4 they would suffer if Prosper's data security systems were breached. Such consequences include the
5 significant costs imposed on Plaintiff and Class Members due to the unauthorized exposure of their
6 Private Information to criminal actors. Nevertheless, Prosper failed to take adequate cybersecurity
7 measures to prevent the Data Breach or the foreseeable injuries it caused.
8

9 43. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class
10 Members' Private Information compromised therein would be targeted by hackers and
11 cybercriminals, for use in variety of different injurious ways. Indeed, the cybercriminals who
12 possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or
13 open fraudulent credit card accounts in Plaintiff's and Class Members' names.
14

15 44. Prosper was, or should have been, fully aware of the unique type and the significant
16 volume of data on Prosper's network server(s) and systems and the significant number of
17 individuals who would be harmed by the exposure of the unencrypted data.
18

19 45. Plaintiff and Class Members were the foreseeable and probable victims of Prosper's
20 inadequate security practices and procedures. Prosper knew or should have known of the inherent
21 risks in collecting and storing the Private Information and the critical importance of providing
22 adequate security for that data, particularly due to the highly public trend of data breach incidents
23 in recent years.
24

25 ***D. Prosper Failed to Comply with FTC Guidelines***

26 46. The Federal Trade Commission ("FTC") has promulgated numerous guides for
27 businesses which highlight the importance of implementing reasonable data security practices.
28

1 According to the FTC, the need for data security should be factored into all business decision
2 making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and
3 appropriate data security for consumers' sensitive personal information is an "unfair practice" in
4 violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.,*
5 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
6

7 47. In October 2016, the FTC updated its publication, *Protecting Personal Information:*
8 *A Guide for Business*, which established cybersecurity guidelines for businesses.³ The guidelines
9 note that businesses should protect the personal customer information that they keep, properly
10 dispose of personal information that is no longer needed, encrypt information stored on computer
11 networks, understand their network's vulnerabilities, and implement policies to correct any security
12 problems. The guidelines also recommend that businesses use an intrusion detection system to
13 expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone
14 is attempting to hack into the system, watch for large amounts of data being transmitted from the
15 system, and have a response plan ready in the event of a breach.
16

17 48. The FTC further recommends that companies not maintain personally identifiable
18 information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive
19 data, require complex passwords to be used on networks, use industry-tested methods for security,
20 monitor the network for suspicious activity, and verify that third-party service providers have
21 implemented reasonable security measures.
22

23 49. The FTC has brought enforcement actions against businesses for failing to
24 adequately and reasonably protect customer data by treating the failure to employ reasonable and
25

26
27 ³ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (October 2016), available at
28 https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited
on Sept. 18, 2025).

1 appropriate measures to protect against unauthorized access to confidential consumer data as an
2 unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq.* Orders resulting
3 from these actions further clarify the measures businesses must take to meet their data security
4 obligations.

5
6 50. Such FTC enforcement actions include those against businesses that fail to
7 adequately protect customer data, like Prosper here. *See, e.g., In the Matter of LabMD, Inc.*, 2016-
8 2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he
9 Commission concludes that LabMD’s data security practices were unreasonable and constitute an
10 unfair act or practice in violation of Section 5 of the FTC Act.”).

11
12 51. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
13 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice
14 by businesses like Prosper of failing to use reasonable measures to protect Private Information they
15 collect and maintain from consumers. The FTC publications and orders described above also form
16 part of the basis of Prosper’s duty in this regard.

17
18 52. The FTC has also recognized that personal data is a new and valuable form of
19 currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated
20 that “most consumers cannot begin to comprehend the types and amount of information collected
21 by businesses, or why their information may be commercially valuable. Data is currency. The larger
22 the data set, the greater potential for analysis and profit.”⁴

23
24 53. As evidenced by the Data Breach, Prosper failed to properly implement basic data
25 security practices. Prosper’s failure to employ reasonable and appropriate measures to protect

26
27 ⁴ FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009),
28 transcript available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on Sept. 18, 2025).

1 against unauthorized access to Plaintiff’s and Class Members’ Private Information constitutes an
2 unfair act or practice prohibited by Section 5 of the FTCA.

3 54. Prosper was at all times fully aware of its obligation to protect the Private
4 Information of its customers yet failed to comply with such obligations. Defendant was also aware
5 of the significant repercussions that would result from its failure to do so.
6

7 ***E. Prosper Failed to Comply with Industry Standards***

8 55. As noted above, experts studying cybersecurity routinely identify businesses as
9 being particularly vulnerable to cyberattacks because of the value of the Private Information which
10 they collect and maintain.

11 56. The Center for Internet Security’s (CIS) Critical Security Controls (CSC)
12 recommends certain best practices to adequately secure data and prevent cybersecurity attacks,
13 including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and
14 Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and
15 Software, Account Management, Access Control Management, Continuous Vulnerability
16 Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses,
17 Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security
18 Awareness and Skills Training, Service Provider Management, Application Software Security,
19 Incident Response Management, and Penetration Testing.⁵
20
21

22 57. The National Institute of Standards and Technology (“NIST”) also recommends
23 certain practices to safeguard systems, such as the following:
24

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

27 ⁵ *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, [https://www.cisecurity.org/controls/cis-](https://www.cisecurity.org/controls/cis-controls-list)
28 [controls-list](https://www.cisecurity.org/controls/cis-controls-list) (last visited on Sept. 18, 2025).

- 1 b. Use security software to protect data.
- 2 c. Encrypt sensitive data, at rest and in transit.
- 3 d. Conduct regular backups of data.
- 4 e. Update security software regularly, automating those updates if
- 5 possible.
- 6 f. Have formal policies for safely disposing of electronic files and old
- 7 devices.
- 8 g. Train everyone who uses your computers, devices, and network
- 9 about cybersecurity. You can help employees understand their
- 10 personal risk in addition to their crucial role in the workplace.

11 58. Further still, the United States Cybersecurity and Infrastructure Security Agency
12 (“CISA”) makes specific recommendations to organizations to guard against cybersecurity attacks,
13 including (a) reducing the likelihood of a damaging cyber intrusion by validating that “remote
14 access to the organization’s network and privileged or administrative access requires multi-factor
15 authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known
16 exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization’s IT personnel
17 have disabled all ports and protocols that are not essential for business purposes,” and other steps;
18 (b) taking steps to quickly detect a potential intrusion, including “[e]nsur[ing] that cybersecurity/IT
19 personnel are focused on identifying and quickly assessing any unexpected or unusual network
20 behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing]
21 that the organization's entire network is protected by antivirus/antimalware software and that
22 signatures in these tools are updated,” and (c) “[e]nsur[ing] that the organization is prepared to
23 respond if an intrusion occurs,” and other steps.⁶

24
25
26
27 ⁶ *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY,
28 <https://www.cisa.gov/shields-guidance-organizations> (last visited Sept. 18, 2025).

1 59. Defendant failed to implement industry-standard cybersecurity measures, including
2 by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0
3 (including PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-
4 DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-
5 06, DE.CM-09, and RS.CO-04) and the Center for Internet Security’s Critical Security Controls
6 (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing
7 to comply with other industry standards for protecting Plaintiff’s and Class Members’ Private
8 Information, resulting in the Data Breach.
9

10 ***F. Prosper Breached its Duty to Safeguard Plaintiff’s and Class Members’ Private***
11 ***Information***

12
13 60. In addition to its obligations under federal and state laws, Prosper owed a duty to
14 Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing,
15 safeguarding, deleting, and protecting the Private Information in its possession from being
16 compromised, lost, stolen, accessed, and misused by unauthorized persons. Prosper owed a duty to
17 Plaintiff and Class Members to provide reasonable security, including complying with industry
18 standards and requirements, training for its staff, and ensuring that its computer systems, networks,
19 and protocols adequately protected the Private Information of Class Members
20

21 61. Prosper breached its obligations to Plaintiff and Class Members and/or was
22 otherwise negligent and reckless because it failed to properly maintain and safeguard its computer
23 systems and data. Prosper’s unlawful conduct includes, but is not limited to, the following acts
24 and/or omissions:

- 25 a. Failing to maintain an adequate data security system that would reduce the risk of
26 data breaches and cyberattacks;
27
28 b. Failing to adequately protect customers’ Private Information;

- 1 c. Failing to properly monitor its own data security systems for existing intrusions;
- 2 d. Failing to sufficiently train its employees regarding the proper handling of its
- 3 customers Private Information;
- 4 e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the
- 5 FTCA;
- 6 f. Failing to adhere to industry standards for cybersecurity as discussed above; and
- 7 g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class
- 8 Members' Private Information.
- 9

10 62. Prosper negligently and unlawfully failed to safeguard Plaintiff's and Class
11 Members' Private Information by allowing cyberthieves to access its computer network and
12 systems which contained unsecured and unencrypted Private Information.

13 63. Had Prosper remedied the deficiencies in its information storage and security
14 systems, followed industry guidelines, and adopted security measures recommended by experts in
15 the field, it could have prevented intrusion into its information storage and security systems and,
16 ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

17 64. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's
18 more, they have been harmed as a result of the Data Breach and now face an increased risk of future
19 harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also
20 lost the benefit of the bargain they made with Prosper.

21
22
23 ***G. As a result of the Data Breach, Plaintiff's and Class Members Are at a Significantly***
24 ***Increased Risk of Fraud and Identity Theft.***

25 65. The FTC hosted a workshop to discuss "informational injuries," which are injuries
26 that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as
27
28

1 data breaches or unauthorized disclosure of data.⁷ Exposure of highly sensitive personal
2 information that a consumer wishes to keep private may cause harm to the consumer, such as the
3 ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them
4 of the benefits provided by the full range of goods and services available which can have negative
5 impacts on daily life.

6
7 66. Any victim of a data breach is exposed to serious ramifications regardless of the
8 nature of the data that was breached. Indeed, the reason why criminals steal information is to
9 monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity
10 thieves who desire to extort and harass victims or to take over victims' identities in order to engage
11 in illegal financial transactions under the victims' names.

12
13 67. Because a person's identity is akin to a puzzle, the more accurate pieces of data an
14 identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or
15 to otherwise harass or track the victim. For example, armed with just a name and date of birth, a
16 data thief can utilize a hacking technique referred to as "social engineering" to obtain even more
17 information about a victim's identity, such as a person's login credentials or Social Security
18 number. Social engineering is a form of hacking whereby a data thief uses previously acquired
19 information to manipulate individuals into disclosing additional confidential or personal
20 information through means such as spam phone calls and text messages or phishing emails.

21
22 68. In fact, as technology advances, computer programs may scan the Internet with a
23 wider scope to create a mosaic of information that may be used to link compromised information
24 to an individual in ways that were not previously possible. This is known as the "mosaic effect."

25
26
27 ⁷ *FTC Information Injury Workshop, BE and BCP Staff Perspective*, FEDERAL TRADE COMMISSION (Oct. 2018),
28 available at https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Sept. 18, 2025).

1 Names and dates of birth, combined with contact information like telephone numbers and email
2 addresses, are very valuable to hackers and identity thieves as it allows them to access users' other
3 accounts.

4 69. Thus, even if certain information was not purportedly involved in the Data Breach,
5 the unauthorized parties could use Plaintiff's and Class Members' Private Information to access
6 accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide
7 variety of fraudulent activity against Plaintiff and Class Members.
8

9 70. One such example of how malicious actors may compile Private Information is
10 through the development of "Fullz" packages.
11

12 71. Cybercriminals can cross-reference two sources of the Private Information
13 compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen
14 data with an astonishingly complete scope and degree of accuracy in order to assemble complete
15 dossiers on individuals. These dossiers are known as "Fullz" packages.
16

17 72. The development of "Fullz" packages means that the stolen Private Information
18 from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's
19 phone numbers, email addresses, and other sources and identifiers. In other words, even if certain
20 information such as emails, phone numbers, or credit card or financial account numbers may not
21 be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz
22 package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and
23 scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of
24 the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find
25 that Plaintiff and other Class Members' stolen Private Information are being misused, and that such
26 misuse is fairly traceable to the Data Breach.
27
28

1 73. For these reasons, the FTC recommends that identity theft victims take several time-
2 consuming steps to protect their personal and financial information after a data breach, including
3 contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud
4 alert that lasts for 7 years if someone steals the victim’s identity), reviewing their credit reports,
5 contacting companies to remove fraudulent charges from their accounts, placing a freeze on their
6 credit, and correcting their credit reports.⁸ However, these steps do not guarantee protection from
7 identity theft but can only mitigate identity theft’s long-lasting negative impacts.
8

9 74. Identity thieves can also use stolen personal information such as Social Security
10 numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to
11 obtain a driver’s license or official identification card in the victim’s name but with the thief’s
12 picture, to obtain government benefits, or to file a fraudulent tax return using the victim’s
13 information. In addition, identity thieves may obtain a job using the victim’s Social Security
14 number, rent a house in the victim’s name, receive medical services in the victim’s name, and even
15 give the victim’s personal information to police during an arrest resulting in an arrest warrant being
16 issued in the victim’s name.
17

18 75. PII is data that can be used to detect a specific individual. PII is a valuable property
19 right. Its value is axiomatic, considering the value of big data in corporate America and the
20 consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-
21 reward analysis illustrates beyond doubt that PII has considerable market value.
22
23
24
25
26

27 ⁸ See *IdentityTheft.gov*, FEDERAL TRADE COMMISSION, available at: <https://www.identitytheft.gov/Steps> (last visited
28 on Sept. 18, 2025).

1 76. The U.S. Attorney General stated in 2020 that consumers’ sensitive personal
2 information commonly stolen in data breaches “has economic value.”⁹ The increase in
3 cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to
4 the public and to anyone in Defendant’s industry.

5
6 77. The PII of consumers remains of high value to criminals, as evidenced by the prices
7 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
8 credentials. For example, PII can be sold at a price ranging from \$40 to \$200, and bank details have
9 a price range of \$50 to \$200.¹⁰ Experian reports that a stolen credit or debit card number can sell
10 for \$5 to \$110 on the dark web and that the “fullz” (a term criminals who steal credit card
11 information use to refer to a complete set of information on a fraud victim) sold for \$30 in 2017.¹¹
12

13 78. The Dark Web Price Index of 2023, published by PrivacyAffairs, shows how
14 valuable just email addresses alone can be, even when not associated with a financial account:¹²

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	\$120
600,000 New Zealand email addresses	\$110
2,400,000 million Canada email addresses	\$100

15
16
17
18
19
20
21
22 ⁹ See Attorney General William P. Barr Announces Indictment of Four Members of China’s Military for Hacking into Equifax, U.S. DEP’T OF JUSTICE (Feb. 10, 2020), <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military> (last visited on Sept. 18, 2025).

23 ¹⁰ Your personal data is for sale on the dark web. Here’s how much it costs, DIGITAL TRENDS (Oct. 16, 2019), available
24 at <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs> (last visited on
25 Sept. 18, 2025).

26 ¹¹ Here’s How Much Your Personal Information Is Selling for on the Dark Web, EXPERIAN (Dec. 6, 2017),
<https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web> (last visited on Sept. 18, 2025).

27 ¹² See Dark Web Price Index 2023, PRIVACY AFFAIRS, <https://www.privacyaffairs.com/dark-web-price-index-2023/>
28 (last visited on Sept. 18, 2025).

1 79. Beyond using email addresses for hacking, the sale of a batch of illegally obtained
2 email addresses can lead to increased spam emails. If an email address is swamped with spam, that
3 address may become cumbersome or impossible to use, making it less valuable to its owner.

4 80. Likewise, the value of PII is increasingly evident in our digital economy. Many
5 companies, including Prosper, collect PII for purposes of data analytics and marketing. These
6 companies, collect it to better target customers, and shares it with third parties for similar
7 purposes.¹³

9 81. One author has noted: “Due, in part, to the use of PII in marketing decisions,
10 commentators are conceptualizing PII as a commodity. Individual data points have concrete value,
11 which can be traded on what is becoming a burgeoning market for PII.”¹⁴

12 82. Consumers also recognize the value of their personal information and offer it in
13 exchange for goods and services. The value of PII can be derived not only by a price at which
14 consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive
15 from being able to use it and control the use of it.

17 83. A consumer’s ability to use their PII is encumbered when their identity or credit
18 profile is infected by misuse or fraud. For example, a consumer with false or conflicting information
19 on their credit report may be denied credit. Also, a consumer may be unable to open an electronic
20 account where their email address is already associated with another user. In this sense, among
21 others, the theft of PII in the Data Breach led to a diminution in value of the PII.
22

23
24
25
26 ¹³ See *Privacy Policy*, ROBINHOOD, <https://robinhood.com/us/en/support/articles/privacy-policy/> (last visited on Sept. 18, 2025).

27 ¹⁴ See John T. Soma, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (‘PII’) Equals the*
28 *“Value” of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

1 84. Data breaches, like that at issue here, damage consumers by interfering with their
2 fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to
3 participate in the economic marketplace.

4 85. The Identity Theft Resource Center documents the multitude of harms caused by
5 fraudulent use of PII in its 2023 Consumer Impact Report.¹⁵ After interviewing over 14,000 identity
6 crime victims, researchers found that as a result of the criminal misuse of their PII:
7

- 8 • 77-percent experienced financial-related problems;
- 9 • 29-percent experienced financial losses exceeding \$10,000;
- 10 • 40-percent were unable to pay bills;
- 11 • 28-percent were turned down for credit or loans;
- 12 • 37-percent became indebted;
- 13 • 87-percent experienced feelings of anxiety;
- 14 • 67-percent experienced difficulty sleeping; and
- 15 • 51-percent suffered from panic of anxiety attacks.¹⁶

16 86. It must also be noted that there may be a substantial time lag between when harm
17 occurs and when it is discovered, and also between when PII and/or personal financial information
18 is stolen and when it is used. According to the U.S. Government Accountability Office, which
19 conducted a study regarding data breaches:¹⁷

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

26 ¹⁵ 2023 Consumer Impact Report (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, available online at:
27 https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last
28 visited on [Sept. 18, 2025](#)).

¹⁶ *Id* at pp 21-25.

¹⁷ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), available at <https://www.gao.gov/assets/gao-07-737.pdf> (last visited on [Sept. 18, 2025](#)).

1
2 87. PII is such a valuable commodity to identity thieves that once the information has
3 been compromised, criminals often trade the information on the “cyber black market” for years.

4 88. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity
5 theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to
6 vigilantly monitor their accounts for many years to come.

7
8 **V. PLAINTIFF’S AND CLASS MEMBERS’ DAMAGES**

9 ***Plaintiff Billy Yoder’s Experience***

10 89. Plaintiff Yoder is a customer of Prosper.

11 90. When Plaintiff Yoder first became a customer, Defendant required that he provide
12 it with substantial amounts of his PII.

13 91. On or about September 17, 2025, Plaintiff Yoder received the Notice informing him
14 that his Private Information had been involved during the Data Breach. The Notice provided that
15 the Private Information compromised included “certain personal information, including Social
16 Security numbers.”

17
18 92. The Notice offered Plaintiff Yoder limited credit monitoring services, which is not
19 sufficient given that Plaintiff Yoder will now experience a lifetime of increased risk of identity theft
20 and other forms of targeted fraudulent misuse of his Private Information.

21 93. Plaintiff Yoder suffered actual injury in the form of time spent dealing with the Data
22 Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his
23 accounts for fraud.

24
25 94. Plaintiff Yoder would not have provided his Private Information to Defendant had
26 Defendant timely disclosed that its systems lacked adequate computer and data security practices
27
28

1 to safeguard its customers' personal information from theft, and that those systems were subject to
2 a data breach.

3 95. Plaintiff Yoder suffered actual injury in the form of having his Private Information
4 compromised and/or stolen as a result of the Data Breach.

5 96. Plaintiff Yoder suffered actual injury in the form of damages to and diminution in
6 the value of his personal and potentially financial information – a form of intangible property that
7 Plaintiff Yoder entrusted to Defendant for the purpose of receiving peer-to-peer lending services
8 from Defendant and which was compromised in, and as a result of, the Data Breach.

9 97. Plaintiff Yoder suffered imminent and impending injury arising from the
10 substantially increased risk of future fraud, identity theft, and misuse posed by his Private
11 Information being placed in the hands of criminals.

12 98. Plaintiff Yoder has a continuing interest in ensuring that his Private Information,
13 which remains in the possession of Defendant, is protected and safeguarded from future breaches.
14 This interest is particularly acute, as Defendant's systems have already been shown to be
15 susceptible to compromise and are subject to further attack so long as Defendant fails to undertake
16 the necessary and appropriate security and training measures to protect its customers' Private
17 Information

18 99. As a result of the Data Breach, Plaintiff Yoder made reasonable efforts to mitigate
19 the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing
20 financial accounts for any indications of actual or attempted identity theft or fraud, and researching
21 the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will
22 now need to use. Plaintiff Yoder has spent several hours dealing with the Data Breach, valuable
23 time he otherwise would have spent on other activities.

1 100. As a result of the Data Breach, Plaintiff Yoder has suffered anxiety as a result of the
2 release of his Private Information to cybercriminals, which Private Information he believed would
3 be protected from unauthorized access and disclosure. These feelings include anxiety about
4 unauthorized parties viewing, selling, and/or using his Private Information for purposes of
5 committing cyber and other crimes against him. Plaintiff Yoder is very concerned about this
6 increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud
7 resulting from the Data Breach will have on his life.

9 101. Plaintiff Yoder also suffered actual injury as a result of the Data Breach in the form
10 of (a) damage to and diminution in the value of his Private Information, a form of property that
11 Defendant obtained from Plaintiff Yoder; (b) violation of his privacy rights; and (c) present,
12 imminent, and impending injury arising from the increased risk of identity theft, and fraud he now
13 faces.

15 102. As a result of the Data Breach, Plaintiff Yoder anticipates spending considerable
16 time and money on an ongoing basis to try to mitigate and address the many harms caused by the
17 Data Breach.

18 103. In sum, Plaintiff and Class Members have been damaged by the compromise of their
19 Private Information in the Data Breach.

21 104. Plaintiff and Class Members entrusted their Private Information to Defendant in
22 order to receive Defendant's lending services.

23 105. Plaintiff's Private Information was subsequently compromised as a direct and
24 proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data
25 security practices.

26 106. As a direct and proximate result of Prosper's actions and omissions, Plaintiff and
27 Class Members have been harmed and are at an imminent, immediate, and continuing increased
28

1 risk of harm, including but not limited to, loans opened in their names, tax returns filed in their
2 names, utility bills opened in their names, credit card accounts opened in their names, and other
3 forms of identity theft.

4 107. Further, as a direct and proximate result of Prosper’s conduct, Plaintiff and Class
5 Members have been forced to spend time dealing with the effects of the Data Breach.

6 108. Plaintiff and Class Members also face a substantial risk of being targeted in future
7 phishing, data intrusion, and other illegal schemes through the misuse of their Private Information,
8 since potential fraudsters will likely use such Private Information to carry out such targeted schemes
9 against Plaintiff and Class Members.
10

11 109. The Private Information maintained by and stolen from Defendant’s systems,
12 combined with publicly available information, allows nefarious actors to assemble a detailed
13 mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent
14 schemes against Plaintiff and Class Members.
15

16 110. Plaintiff and Class Members also lost the benefit of the bargain they made with
17 Prosper. Plaintiff and Class Members overpaid for services that were intended to be accompanied
18 by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid
19 to Prosper was intended to be used by Prosper to fund adequate security of Prosper’s system and
20 protect Plaintiff’s and Class Members’ Private Information. Thus, Plaintiff and the Class did not
21 receive what they paid for.
22

23 111. Additionally, as a direct and proximate result of Prosper’s conduct, Plaintiff and
24 Class Members have also been forced to take the time and effort to mitigate the actual and potential
25 impact of the data breach on their everyday lives, including placing “freezes” and “alerts” with
26 credit reporting agencies, contacting their financial institutions, closing or modifying financial
27
28

1 accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized
2 activity for years to come.

3 112. Plaintiff and Class Members may also incur out-of-pocket costs for protective
4 measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs
5 directly or indirectly related to the Data Breach.
6

7 113. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII
8 and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have
9 recognized the propriety of loss of value damages in related cases. An active and robust legitimate
10 marketplace for Private Information also exists. In 2019, the data brokering industry was worth
11 roughly \$200 billion.¹⁸ In fact, consumers who agree to provide their web browsing history to the
12 Nielsen Corporation can in turn receive up to \$50 a year.¹⁹
13

14 114. As a result of the Data Breach, Plaintiff's and Class Members' Private Information,
15 which has an inherent market value in both legitimate and illegal markets, has been harmed and
16 diminished due to its acquisition by cybercriminals. This transfer of valuable information happened
17 with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic
18 loss. Moreover, the Private Information is apparently readily available to others, and the rarity of
19 the Private Information has been destroyed because it is no longer only held by Plaintiff and the
20 Class Members, and because that data no longer necessarily correlates only with activities
21 undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.
22

23 115. Plaintiff and Class Members were also damaged via benefit-of-the-bargain
24 damages. The contractual bargain entered into between Plaintiff and Defendant included
25

26 ¹⁸ See *How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD,
<https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/> (last visited on Sept. 18, 2025).

27 ¹⁹ *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL,
28 <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last visited on Sept. 18, 2025).

1 Defendant's contractual obligation to provide adequate data security, which Defendant failed to
2 provide. Thus, Plaintiff and Class Members did not get what they bargained for.

3 116. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a
4 direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value
5 of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses
6 include, but are not limited to, the following:
7

- 8 a. Monitoring for and discovering fraudulent charges;
- 9 b. Addressing their inability to withdraw funds linked to compromised accounts;
- 10 c. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- 11 d. Contacting financial institutions and closing or modifying financial accounts;
- 12 and
- 13 e. Closely reviewing and monitoring bank accounts and credit reports for
14 additional unauthorized activity for years to come.
15

16 117. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private
17 Information, which is believed to still be in the possession of Prosper, is protected from future
18 additional breaches by the implementation of more adequate data security measures and safeguards,
19 including but not limited to, ensuring that the storage of data or documents containing personal and
20 financial information is not accessible online, that access to such data is password-protected, and
21 that such data is properly encrypted.
22

23 118. As a direct and proximate result of Prosper's actions and inactions, Plaintiff and
24 Class Members have suffered a loss of privacy and have suffered cognizable harm, including an
25 imminent and substantial future risk of harm, in the forms set forth above.
26

27 **VI. CLASS ACTION ALLEGATIONS**

1 119. Plaintiff brings this action individually and on behalf of all other persons similarly
2 situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

3 120. Specifically, Plaintiff proposes the following Nationwide Class (referred to herein
4 as the “Class”), subject to amendment as appropriate:

5
6 **Nationwide Class**

7 All individuals in the United States who had Private Information
8 impacted as a result of the Data Breach, including all who were sent
a notice of the Data Breach.

9 121. Excluded from the Class are Defendant and its parents or subsidiaries, any entities
10 in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives,
11 heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is
12 assigned as well as their judicial staff and immediate family members.

13
14 122. Plaintiff reserves the right to modify or amend the definitions of the proposed
15 Nationwide Class, as well as the addition of any subclasses, before the Court determines whether
16 certification is appropriate.

17 123. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a),
18 (b)(2), and (b)(3).

19 124. **Numerosity.** The Class Members are so numerous that joinder of all members is
20 impracticable. Though the exact number and identities of Class Members are unknown at this time,
21 based on information and belief, the Class consists of nationwide customers of Prosper whose data
22 was compromised in the Data Breach. The identities of Class Members are ascertainable through
23 Prosper’s records, Class Members’ records, publication notice, self-identification, and other means.
24

25 125. **Commonality.** There are questions of law and fact common to the Class which
26 predominate over any questions affecting only individual Class Members. These common
27 questions of law and fact include, without limitation:
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- a. Whether Prosper engaged in the conduct alleged herein;
- b. When Prosper learned of the Data Breach;
- c. Whether Prosper’s response to the Data Breach was adequate;
- d. Whether Prosper unlawfully lost or disclosed Plaintiff’s and Class Members’ Private Information;
- e. Whether Prosper failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- f. Whether Prosper’s data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- g. Whether Prosper’s data security systems prior to and during the Data Breach were consistent with industry standards;
- h. Whether Prosper owed a duty to Class Members to safeguard their Private Information;
- i. Whether Prosper breached its duty to Class Members to safeguard their Private Information;
- j. Whether hackers obtained Class Members’ Private Information via the Data Breach;
- k. Whether Prosper had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- l. Whether Prosper breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- m. Whether Prosper knew or should have known that its data security systems and monitoring processes were deficient;

- n. What damages Plaintiff and Class Members suffered as a result of Prosper's misconduct;
- o. Whether Prosper's conduct was negligent;
- p. Whether Prosper's conduct was *per se* negligent;
- q. Whether Prosper was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

126. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

127. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

128. **Predominance.** Prosper has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Prosper's 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.

1 133. Prosper knowingly collected, came into possession of, and maintained Plaintiff's
2 and Class Members' Private Information, and had a duty to exercise reasonable care in
3 safeguarding, securing, and protecting such Information from being disclosed, compromised, lost,
4 stolen, and misused by unauthorized parties.

5
6 134. Prosper knew or should have known of the risks inherent in collecting the Private
7 Information of Plaintiff and Class Members and the importance of adequate security. Prosper was
8 on notice because, on information and belief, it knew or should have known that it would be an
9 attractive target for cyberattacks.

10 135. Prosper owed a duty of care to Plaintiff and Class Members whose Private
11 Information was entrusted to it. Prosper's duties included, but were not limited to, the following:

- 12 a. To exercise reasonable care in obtaining, retaining, securing, safeguarding,
13 deleting, and protecting Private Information in its possession;
- 14 b. To protect customers' Private Information using reasonable and adequate
15 security procedures and systems compliant with industry standards;
- 16 c. To have procedures in place to prevent the loss or unauthorized dissemination
17 of Private Information in its possession;
- 18 d. To employ reasonable security measures and otherwise protect the Private
19 Information of Plaintiff and Class Members pursuant to the FTCA;
- 20 e. To implement processes to quickly detect a data breach and to timely act on
21 warnings about data breaches; and
- 22 f. To promptly notify Plaintiff and Class Members of the Data Breach, and to
23 precisely disclose the type(s) of information compromised.

24
25 136. Prosper's duty to employ reasonable data security measures arose, in part, under
26 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .
27
28

1 practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair
2 practice of failing to use reasonable measures to protect confidential data.

3 137. Prosper’s duty also arose because Defendant was bound by industry standards to
4 protect its customers’ confidential Private Information.

5 138. Plaintiff and Class Members were foreseeable victims of any inadequate security
6 practices on the part of Defendant, and Prosper owed them a duty of care to not subject them to an
7 unreasonable risk of harm.
8

9 139. Prosper, through its actions and/or omissions, unlawfully breached its duty to
10 Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding
11 Plaintiff’s and Class Members’ Private Information within Prosper’s possession.

12 140. Prosper, by its actions and/or omissions, breached its duty of care by failing to
13 provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and
14 data security practices to safeguard the Private Information of Plaintiff and Class Members.
15

16 141. Prosper, by its actions and/or omissions, breached its duty of care by failing to
17 promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to
18 the persons whose Private Information was compromised.

19 142. Prosper breached its duties, and thus was negligent, by failing to use reasonable
20 measures to protect Class Members’ Private Information. The specific negligent acts and omissions
21 committed by Defendant include, but are not limited to, the following:
22

- 23 a. Failing to adopt, implement, and maintain adequate security measures to safeguard
24 Class Members’ Private Information;
- 25 b. Failing to adequately monitor the security of its networks and systems;
- 26 c. Failing to periodically ensure that its email system maintained reasonable data
27 security safeguards;
28

- 1 d. Allowing unauthorized access to Class Members' Private Information;
- 2 e. Failing to comply with the FTCA; and
- 3 f. Failing to detect in a timely manner that Class Members' Private Information had
- 4 been compromised.

5
6 143. Prosper had a special relationship with Plaintiff and Class Members. Plaintiff's and
7 Class Members' willingness to entrust Prosper with their Private Information was predicated on the
8 understanding that Prosper would take adequate security precautions. Moreover, only Prosper had
9 the ability to protect its systems (and the Private Information that it stored on them) from attack.

10 144. Prosper's breach of duties owed to Plaintiff and Class Members caused Plaintiff's
11 and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

12 145. As a result of Prosper's ongoing failure to notify Plaintiff and Class Members
13 regarding exactly what Private Information has been compromised, Plaintiff and Class Members
14 have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

15 146. Prosper's breaches of duty also caused a substantial, imminent risk to Plaintiff and
16 Class Members of identity theft, loss of control over their Private Information, and/or loss of time
17 and money to monitor their accounts for fraud.

18 147. As a result of Prosper's negligence in breach of its duties owed to Plaintiff and Class
19 Members, Plaintiff and Class Members are in danger of imminent harm in that their Private
20 Information, which is still in the possession of third parties, will be used for fraudulent purposes.

21 148. Prosper also had independent duties under state laws that required it to reasonably
22 safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the
23 Data Breach.

24 149. As a direct and proximate result of Prosper's negligent conduct, Plaintiff and Class
25 Members have suffered damages as alleged herein and are at imminent risk of further harm.
26
27
28

1 150. The injury and harm that Plaintiff and Class Members suffered was reasonably
2 foreseeable.

3 151. Plaintiff and Class Members have suffered injury and are entitled to damages in an
4 amount to be proven at trial.

5 152. In addition to monetary relief, Plaintiff and Class Members are also entitled to
6 injunctive relief requiring Prosper to, *inter alia*, strengthen its data security systems and monitoring
7 procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and
8 identity theft insurance to Plaintiff and Class Members.

9
10 **COUNT II**
11 **NEGLIGENCE *PER SE***
12 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

13 153. Plaintiff restates and realleges all of the allegations stated above and hereafter as if
14 fully set forth herein.

15 154. Pursuant to Section 5 of the FTCA, Prosper had a duty to provide fair and adequate
16 computer systems and data security to safeguard the Private Information of Plaintiff and Class
17 Members.

18 155. Prosper breached its duties by failing to employ industry-standard cybersecurity
19 measures in order to comply with the FTCA, including but not limited to proper segregation, access
20 controls, password protection, encryption, intrusion detection, secure destruction of unnecessary
21 data, and penetration testing.

22 156. Plaintiff and Class Members are within the class of persons that the FTCA is
23 intended to protect.

24 157. The FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as
25 interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures
26 to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings
27
28

1 and publications described above, together with the industry-standard cybersecurity measures set
2 forth herein, form part of the basis of Prosper's duty in this regard.

3 158. Prosper violated the FTCA by failing to use reasonable measures to protect the
4 Private Information of Plaintiff and the Class and by not complying with applicable industry
5 standards, as described herein.
6

7 159. It was reasonably foreseeable, particularly given the growing number of data
8 breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and
9 Class Members' Private Information in compliance with applicable laws would result in an
10 unauthorized third-party gaining access to Prosper's networks, databases, and computers that stored
11 Plaintiff's and Class Members' unencrypted Private Information.
12

13 160. Prosper's violations of the FTCA constitute negligence *per se*.

14 161. Plaintiff's and Class Members' Private Information constitutes personal property
15 that was stolen due to Prosper's negligence, resulting in harm, injury, and damages to Plaintiff and
16 Class Members.

17 162. As a direct and proximate result of Prosper's negligence *per se*, Plaintiff and the
18 Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized
19 access of their Private Information, including but not limited to damages from the lost time and
20 effort to mitigate the actual and potential impact of the Data Breach on their lives.
21

22 163. Prosper breached its duties to Plaintiff and the Class under the FTCA by failing to
23 provide fair, reasonable, or adequate computer systems and data security practices to safeguard
24 Plaintiff's and Class Members' Private Information.

25 164. As a direct and proximate result of Prosper's negligent conduct, Plaintiff and Class
26 Members have suffered injury and are entitled to compensatory and consequential damages in an
27 amount to be proven at trial.
28

1 165. In addition to monetary relief, Plaintiff and Class Members are also entitled to
2 injunctive relief requiring Prosper to, *inter alia*, strengthen its data security systems and monitoring
3 procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and
4 identity theft insurance to Plaintiff and Class Members.

5
6 **COUNT III**
7 **BREACH OF CONTRACT**
8 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

9 166. Plaintiff restates and realleges all of the allegations stated above and hereafter as if
10 fully set forth herein.

11 167. Plaintiff and Class Members entered into a valid and enforceable contract through
12 which they paid money to Prosper in exchange for services. That contract included promises by
13 Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private
14 Information.

15 168. Prosper's Privacy Policy memorialized the rights and obligations of Prosper and its
16 customers. This document was provided to Plaintiff and Class Members in a manner in which it
17 became part of the agreement for services.

18 169. In the Privacy Policy, Prosper commits to protecting the privacy and security of
19 private information and promises to never share Plaintiff's and Class Members' Private Information
20 except under certain limited circumstances.

21 170. Plaintiff and Class Members fully performed their obligations under their contracts
22 with Prosper.

23 171. However, Prosper did not secure, safeguard, and/or keep private Plaintiff's and
24 Class Members' Private Information, and therefore Prosper breached its contracts with Plaintiff
25 and Class Members.
26
27
28

1 172. Prosper allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class
2 Members' Private Information without permission. Therefore, Prosper breached the Privacy Policy
3 with Plaintiff and Class Members.

4 173. Prosper's failure to satisfy its confidentiality and privacy obligations resulted in
5 Prosper providing services to Plaintiff and Class Members that were of a diminished value.
6

7 174. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured
8 as described herein, including in Defendant's failure to fully perform its part of the bargain with
9 Plaintiff and Class Members.

10 175. As a direct and proximate result of Prosper's conduct, Plaintiff and Class Members
11 suffered and will continue to suffer damages in an amount to be proven at trial.
12

13 176. In addition to monetary relief, Plaintiff and Class Members are also entitled to
14 injunctive relief requiring Prosper to, *inter alia*, strengthen its data security systems and monitoring
15 procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and
16 identity theft insurance to Plaintiff and Class Members.

17 **COUNT IV**
18 **BREACH OF IMPLIED CONTRACT**
19 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

20 177. Plaintiff restates and realleges all of the allegations stated above and hereafter as if
21 fully set forth herein.

22 178. This Count is pleaded in the alternative to Count III above.

23 179. Prosper provides peer-to-peer lending services to Plaintiff and Class Members.
24 Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of
25 those services through their collective conduct, including by Plaintiff and Class Members paying
26 for services from Defendant.
27
28

1 180. Through Defendant's offering of lending services, it knew or should have known
2 that it must protect Plaintiff's and Class Members' confidential Private Information in accordance
3 with Prosper's policies, practices, and applicable law.

4 181. As consideration, Plaintiff and Class Members paid money to Prosper and turned
5 over valuable Private Information to Prosper. Accordingly, Plaintiff and Class Members bargained
6 with Prosper to securely maintain and store their Private Information.
7

8 182. Prosper accepted possession of Plaintiff's and Class Members' Private Information
9 for the purpose of providing lending services to Plaintiff and Class Members.

10 183. In delivering their Private Information to Prosper and paying for lending services,
11 Plaintiff and Class Members intended and understood that Prosper would adequately safeguard the
12 Private Information as part of that service.

13 184. Defendant's implied promises to Plaintiff and Class Members include, but are not
14 limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also
15 protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that
16 is placed in the control of its employees is restricted and limited to achieve an authorized business
17 purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and
18 implementing appropriate retention policies to protect the Private Information against criminal data
19 breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication
20 for access; and (7) taking other steps to protect against foreseeable data breaches.
21

22 185. Plaintiff and Class Members would not have entrusted their Private Information to
23 Prosper in the absence of such an implied contract.
24

25 186. Had Prosper disclosed to Plaintiff and the Class that they did not have adequate
26 computer systems and security practices to secure sensitive data, Plaintiff and Class Members
27 would not have provided their Private Information to Prosper.
28

1 187. Prosper recognized that Plaintiff's and Class Member's Private Information is
2 highly sensitive and must be protected, and that this protection was of material importance as part
3 of the bargain to Plaintiff and the other Class Members.

4 188. Prosper violated these implied contracts by failing to employ reasonable and
5 adequate security measures to secure Plaintiff's and Class Members' Private Information.
6

7 189. Plaintiff and Class Members have been damaged by Prosper's conduct, including
8 the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

9 **COUNT V**
10 **UNJUST ENRICHMENT**
11 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

12 190. Plaintiff restates and realleges all of the allegations stated above and hereafter as if
13 fully set forth herein.

14 191. This Count is pleaded in the alternative to Counts III and IV above.

15 192. Plaintiff and Class Members conferred a benefit on Prosper by turning over their
16 Private Information to Defendant and by paying for lending services that should have included
17 cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not
18 receive such protection.

19 193. Upon information and belief, Prosper funds its data security measures entirely from
20 its general revenue, including from payments made to it by Plaintiff and Class Members.
21

22 194. As such, a portion of the payments made by Plaintiff and Class Members is to be
23 used to provide a reasonable and adequate level of data security that is in compliance with
24 applicable state and federal regulations and industry standards, and the amount of the portion of
25 each payment made that is allocated to data security is known to Prosper.
26
27
28

1 195. Prosper has retained the benefits of its unlawful conduct, including the amounts of
2 payment received from Plaintiff and Class Members that should have been used for adequate
3 cybersecurity practices that it failed to provide.

4 196. Prosper knew that Plaintiff and Class Members conferred a benefit upon it, which
5 Prosper accepted. Prosper profited from these transactions and used the Private Information of
6 Plaintiff and Class Members for business purposes, while failing to use the payments it received
7 for adequate data security measures that would have secured Plaintiff's and Class Members' Private
8 Information and prevented the Data Breach.

9 197. If Plaintiff and Class Members had known that Prosper had not adequately secured
10 their Private Information, they would not have agreed to provide such Private Information to
11 Defendant.

12 198. Due to Prosper's conduct alleged herein, it would be unjust and inequitable under
13 the circumstances for Prosper to be permitted to retain the benefit of its wrongful conduct.

14 199. As a direct and proximate result of Prosper's conduct, Plaintiff and Class Members
15 have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to
16 control how their Private Information is used; (ii) the compromise, publication, and/or theft of their
17 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and
18 recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost
19 opportunity costs associated with effort expended and the loss of productivity addressing and
20 attempting to mitigate the actual and future consequences of the Data Breach, including but not
21 limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;
22 (v) the continued risk to their Private Information, which remains in Prosper's possession and is
23 subject to further unauthorized disclosures so long as Prosper fails to undertake appropriate and
24 adequate measures to protect Private Information in its continued possession; and (vi) future costs
25
26
27
28

1 in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the
2 impact of the Private Information compromised as a result of the Data Breach for the remainder of
3 the lives of Plaintiff and Class Members.

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

9
10 201. Plaintiff and Class Members may not have an adequate remedy at law against
11 Prosper, and accordingly, they plead this claim for unjust enrichment in addition to, or in the
12 alternative to, other claims pleaded herein.

13
14 **COUNT VI**
15 **DECLARATORY JUDGMENT**
16 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

17 202. Plaintiff restates and realleges all of the allegations stated above and hereafter as if
18 fully set forth herein.

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

23 204. Prosper owes a duty of care to Plaintiff and Class Members, which required it to
24 adequately secure Plaintiff's and Class Members' Private Information.

25 205. Prosper still possesses Private Information regarding Plaintiff and Class Members.

26 206. Plaintiff alleges that Prosper's data security measures remain inadequate.
27 Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their Private
28

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

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

- 5
- 6 a. Prosper owes a legal duty to secure its customers' Private Information and to timely
7 notify customers of a data breach under the common law and Section 5 of the FTCA;
 - 8 b. Prosper's existing security measures do not comply with its explicit or implicit
9 contractual obligations and duties of care to provide reasonable security procedures
10 and practices that are appropriate to protect customers' Private Information; and
 - 11 c. Prosper continues to breach this legal duty by failing to employ reasonable measures
12 to secure customers' Private Information.

13

14 208. This Court should also issue corresponding prospective injunctive relief requiring
15 Prosper to employ adequate security protocols consistent with legal and industry standards to
16 protect customers' Private Information, including the following:

- 17
- 18 a. Order Prosper to provide lifetime credit monitoring and identity theft insurance to
19 Plaintiff and Class Members.
 - 20 b. Order that, to comply with Defendant's explicit or implicit contractual obligations
21 and duties of care, Prosper must implement and maintain reasonable security
22 measures, including, but not limited to:
 - 23 i. engaging third-party security auditors/penetration testers as well as internal
24 security personnel to conduct testing, including simulated attacks,
25 penetration tests, and audits on Prosper's systems on a periodic basis, and
26 ordering Prosper to promptly correct any problems or issues detected by such
27 third-party security auditors;

- 1 ii. engaging third-party security auditors and internal personnel to run
- 2 automated security monitoring;
- 3 iii. auditing, testing, and training its security personnel regarding any new or
- 4 modified procedures;
- 5 iv. segmenting its user applications by, among other things, creating firewalls
- 6 and access controls so that if one area is compromised, hackers cannot gain
- 7 access to other portions of Prosper’s systems;
- 8 v. conducting regular database scanning and security checks;
- 9 vi. routinely and continually conducting internal training and education to
- 10 inform internal security personnel how to identify and contain a breach when
- 11 it occurs and what to do in response to a breach; and
- 12 vii. meaningfully educating its users about the threats they face with regard to
- 13 the security of their Private Information, as well as the steps Prosper’s
- 14 customers should take to protect themselves.
- 15
- 16

17 209. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an
18 adequate legal remedy to prevent another data breach at Prosper. The risk of another such breach
19 is real, immediate, and substantial. If another breach at Prosper occurs, Plaintiff will not have an
20 adequate remedy at law because many of the resulting injuries are not readily quantifiable.

21
22 210. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to
23 Prosper if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity
24 theft and other related damages if an injunction is not issued. On the other hand, the cost of
25 Prosper’s compliance with an injunction requiring reasonable prospective data security measures
26 is relatively minimal, and Prosper has a pre-existing legal obligation to employ such measures.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

IX. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: September 18, 2025

Respectfully submitted,

/s/Catherine Ybarra

Catherine Ybarra (Bar No. 283360)

SIRI & GLIMSTAD LLP

700 S. Flower Street, Suite 1000

Los Angeles, CA 90017

Tel: (213) 297-3807

E: cybarra@sirillp.com

Tyler J. Bean*

Neil P. Williams*

SIRI & GLIMSTAD LLP

745 Fifth Avenue, Suite 500

New York, New York 10151

Tel: (212) 532-1091

E: tbean@sirillp.com

E: nwilliams@sirillp.com

**Pro Hac Vice forthcoming*

Attorneys for Plaintiff and the Putative Class

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

BILLY YODER on behalf of himself and all others similarly situated

(b) County of Residence of First Listed Plaintiff Winston County, AL (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Catherine Ybarra (Bar No. 283360), SIRI & GLIMSTAD LLP, 700 S. Flower Street, Suite 1000, Los Angeles, CA 90017 Tel: (213) 297-3807

DEFENDANTS

PROSPER FUNDING LLC

County of Residence of First Listed Defendant San Francisco County, CA (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

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

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, PTF DEF, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation

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

Table with columns: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes various legal categories like Insurance, Personal Injury, Real Estate, etc.

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

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District (specify), 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. § 1332(d)(2)
Brief description of cause: Plaintiff brings this action against Defendant for their failure to properly secure Plaintiff's private and personal information

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER Please see Exhibit A

DATE 09/18/2025 SIGNATURE OF ATTORNEY OF RECORD /s/Catherine Ybarra

FOR OFFICE USE ONLY RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

EXHIBIT A

RELATED CASES IN THE NORTHERN DISTRICT OF CALIFORNIA:

Chavira, et al. v. Prosper Funding, LLC, 3:25-cv-7958

Mcphee v. Prosper Funding, LLC, 4:25-cv-7947

Walston v. Prosper Funding, LLC, 3:25-cv-7949

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

BILLY YODER on behalf of himself and all others
similarly situated

Plaintiff(s)

v.

PROSPER FUNDING LLC

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) Prosper Funding
221 Main Street, 3rd Floor
San Francisco, CA 94105

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Catherine Ybarra (Bar No. 283360)
SIRI & GLIMSTAD LLP
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 297-3807
E: cybarra@sirillp.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

Signature of Clerk or Deputy Clerk

AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____ .

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____ , who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

I returned the summons unexecuted because _____ ; or

Other *(specify)*:

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00 _____ .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: