Catherine Ybarra (SBN 283360)
cybarra@sirillp.com
Tyler J. Bean (*pro hac vice* to be filed)
tbean@sirillp.com
Neil Williams (*pro hac vice* to be filed)
nwilliams@sirillp.com
SIRI & GLIMSTAD LLP
700 S Flower St, Ste 1000,
Los Angeles, CA 90017
Tel: (213) 297-3807

Jessica A. Wilkes (*pro hac vice* to be filed)
jaw@federmanlaw.com
Federman & Sherwood
10205 N. Pennsylvania Ave
Oklahoma City, OK 73120
Tel: (405) 235-1560

Counsel for Plaintiff and Proposed Lead for the Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOBY CHILDRESS, individually and on behalf of all similarly situated individuals, Plaintiff, v. PROSPER FUNDING, LLC, Defendant.	Case No.: **CLASS ACTION** **CLASS ACTION COMPLAINT FOR DAMAGES** 1. **Negligence** 2. **Negligence *Per Se*** 3. **Breach of Fiduciary Duties** 4. **Breach of Confidence** 5. **Breach of Implied Contract** 6. **Invasion of Privacy** 7. **Injunctive/Declaratory Relief** **JURY TRIAL DEMANDED**

Plaintiff Joby Childress, ("Plaintiff") individually and on behalf of all others similarly situated, brings this action against Defendant Prosper Funding, LLC, ("Prosper") based on personal knowledge and the investigation of counsel, and allege as follows:

I. INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms is caused Plaintiff and thousands of similarly situated persons ("Class" or "Class Members" or "Breach Victims") in a massive and preventable data breach of Defendant's inadequately protected computer network.

2. In September 2025, hackers infiltrated and accessed the inadequately protected computer systems of Defendant and stole the sensitive personal information ("Personal Information" or "PII") of over 17.6 million individuals. Following an investigation, Defendant determined that cybercriminals gained unauthorized access to its systems on (the "Data Breach" or "Breach").

3. The PII taken by the hackers includes: names, addresses, dates of birth, and Social Security numbers.

4. In short, thanks to Defendant's failure to protect the Breach Victims' Personal Information, cyber criminals were able to steal everything they could possibly need to commit nearly every conceivable form of identity theft and wreak havoc on the financial and personal lives of potentially millions of individuals.

5. Defendant is a peer-to-peer lending platform that allows borrowers to access personal loans ranging from $2,000 to $50,000.

6. Defendant's conduct—failing to implement adequate and reasonable measures to ensure their computer systems were protected, failing to take adequate steps to prevent and stop the breach, failing to timely detect the breach, failing to disclose the material facts that they did not have adequate computer systems and security practices to safeguard the Personal Information, failing to honor their repeated promises and representations to protect the Breach Victims' Personal

Information, and failing to provide timely and adequate notice of the Data Breach—caused substantial harm and injuries to Plaintiff and the Class.

7. Plaintiff brings this class action lawsuit on behalf of a nationwide class and state subclasses to hold Defendant responsible for its negligent and reckless failure to use reasonable, current cybersecurity measures to protect class members' Personal Information.

8. Because Defendant presented such a soft target to cybercriminals, Plaintiff and class members have already been subjected to violations of their privacy, fraud, and identity theft, or have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future, spend time to more closely monitor their credit reports, financial accounts, phone lines, and online accounts to guard against identity theft.

9. Plaintiff and Class Members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. On behalf of himself and the Class, Plaintiff seeks actual damages, statutory damages, and punitive damages, with attorney fees, costs, and expenses under negligence, negligence *per se*, breach of fiduciary duties, breach of confidence, breach of implied contract, and invasion of privacy. Plaintiff also seeks injunctive relief, including significant improvements to Defendant's data security systems, future annual audits, and long-term credit monitoring services funded by Defendant, and other remedies as the Court sees fit.

II. THE PARTIES

11. Plaintiff Joby Childress is a citizen of Dalhart, Texas.

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

13. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

14. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

15. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

16. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class, including Plaintiff, are citizens of states different from Defendant.

17. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class members reside in this District.

18. Venue as to Defendant is proper in this judicial district under 28 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

IV. FACTUAL ALLEGATIONS

19. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

A. The Data Breach

20. Defendant sent letters to Plaintiff and the Class Members informing them that, in September 2025, it detected that an unauthorized party had gained remote access to its network, and, following an investigation, it determined that the

unauthorized third party obtained files containing personal information ("Notice of Breach" or "Notice").

21. In spite of the severity of the Data Breach, Defendant has done very little to protect Breach Victims. Defendant is only offering one year of identity monitoring services.

22. Defendant failed to adequately safeguard class members' Personal Information, allowing the cyber criminals to access this wealth of priceless information months before Defendant warned the Breach Victims to be on the lookout.

23. Defendant had obligations created by reasonable industry standards, common law, and their representations to Class Members, to keep their Personal Information confidential and to protect the information from unauthorized access.

24. Plaintiff and Class Members provided their Personal Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

B. Plaintiff's Experience

25. Plaintiff entrusted his Personal Information to Defendant for the purposes of lending.

26. Plaintiff received a letter from Defendant, informing him that his "name and Social Security number" were disclosed to an unknown actor as a result of the Data Breach.

27. Plaintiff has spent hours responding to the Data Breach so far, including reviewing his financial accounts and credit reports.

28. As a result, Plaintiff has spent time responding to the Data Breach, researching and enrolling in credit monitoring and identity theft protection services, reviewing his credit reports, and mitigating fraud and identity theft.

29. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Plaintiff is at imminent risk of severe identity theft and exploitation.

30. Plaintiff is very careful about not sharing his sensitive Personal Information. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

31. Plaintiff stores any document containing his Personal Information in safe and secure locations or destroys such documents. He diligently chooses unique usernames and passwords for her various online accounts.

32. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

33. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

C. Defendant had an Obligation to Protect Personal Information under Federal and State Law and the Applicable Standard of Care

34. Defendant collects, maintains, and stores the Personal Information of Plaintiff and the Class in the usual course of business.

35. In collecting, maintaining, and storing such Personal Information, Defendant promises to such information confidential and protect it from third parties.

36. Defendant was prohibited by the Federal Trade Commission Act (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade

Commission Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

37. Defendant is also required by various state laws and regulations to protect Plaintiff's and Class Members' Personal Information.

38. In addition to its obligations under federal and state laws, Defendant owed a duty to Breach Victims whose Personal Information was entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal Information of the Plaintiff and the Class Members.

39. Defendant owed a duty to Plaintiff and the Class Members whose Personal Information was entrusted to Defendant to design, maintain, and test its computer systems and email system to ensure that the Personal Information in Defendant's possession was adequately secured and protected.

40. Defendant owed a duty to Plaintiff and the Class Members whose Personal Information was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the Personal Information in their possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal Information.

41. Defendant owed a duty to Plaintiff and the Class Members whose Personal Information was entrusted to Defendant to implement processes that would detect a breach on its data security systems in a timely manner.

42. Defendant owed a duty to Plaintiff and the Class Members whose Personal Information was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

43. Defendant owed a duty to Plaintiff and the Class Members whose Personal Information was entrusted to Defendant to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant.

44. Defendant owed a duty to Plaintiff and the Class Members whose Personal Information was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

45. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices.

D. Defendant Was on Notice of Cyber Attack Threats and the Inadequacy of Its Data Security

46. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

47. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[1]

[1] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

48. In April 2020, ZDNet reported, in an article titled “Ransomware mentioned in 1,000+ SEC filings over the past year,” that “[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”[2]

49. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”[3]

50. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting companies such as Defendant and Defendant’s clients, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant and Defendant’s clients, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals’ tactics included threatening to release stolen data.

51. Considering the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII, and Defendant’s type of business had cause to be particularly on guard against such an attack.

---

[2] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

[3] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 25, 2022).

E. Defendant Could Have and Should Have Prevented this Data Breach

52. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

[4] See How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 17, 2023).

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[5]

54. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

[5] *Id.* at 3-4.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[6]

55. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; Remove privilege credentials

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full comprise

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

[6] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited July 17, 2023).

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege

Monitor for adversarial activities

- Hunt for brute force attempts
- Monitor for cleanup of Event logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[7]

56. Given that Defendant was storing the PII of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

F. Plaintiff and the Class Continue to Suffer Harm

57. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[8] Cyber criminals can leverage Plaintiff's and Class Members' Personal Information that was stolen in the Data Breach to commit thousands-indeed, millions-of additional crimes, including opening new financial accounts in Breach Victims' names, taking out loans in Breach Victims' names, using Breach Victims' names to obtain government benefits, using Breach Victims' Personal Information to file fraudulent tax returns, using Breach Victims' information to obtain government benefits, filing fraudulent tax returns using

---

[7] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a- preventable-disaster/ (last visited July 17, 2023).

[8] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

Breach Victims' information, obtaining driver's licenses in Breach Victims' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Breach Victims could be arrested for crimes identity thieves have committed.

58. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

59. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.9 Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.10 Criminals can also purchase access to entire company data breaches from $900 to $4,500.11

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

61. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to

---

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 17, 2023).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July17, 2023).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 17, 2023).

credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."12

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

63. This was a financially motivated data breach, as the only reason the cyber criminals stole Plaintiff's and the Class Members' Personal Information from Defendant was to engage in the kinds of criminal activity described in paragraph 85, which will result, and has already begun to, in devastating financial and personal losses to Breach Victims.

64. This is not just speculative. As the FTC has reported, if hackers get access to Personal Information, they ***will*** use it.[13]

65. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

---

[12] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 17, 2023).

[13] Ari Lazarus, "How fast will identity thieves use stolen info?," May 24, 2017, https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu (emphasis added).

66. For instance, with a stolen social security number, which is part of the Personal Information compromised in the Data Breach, someone can open financial, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[15]

67. One such example of criminals using PII for profit is the development of "Fullz" packages.

68. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

69. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

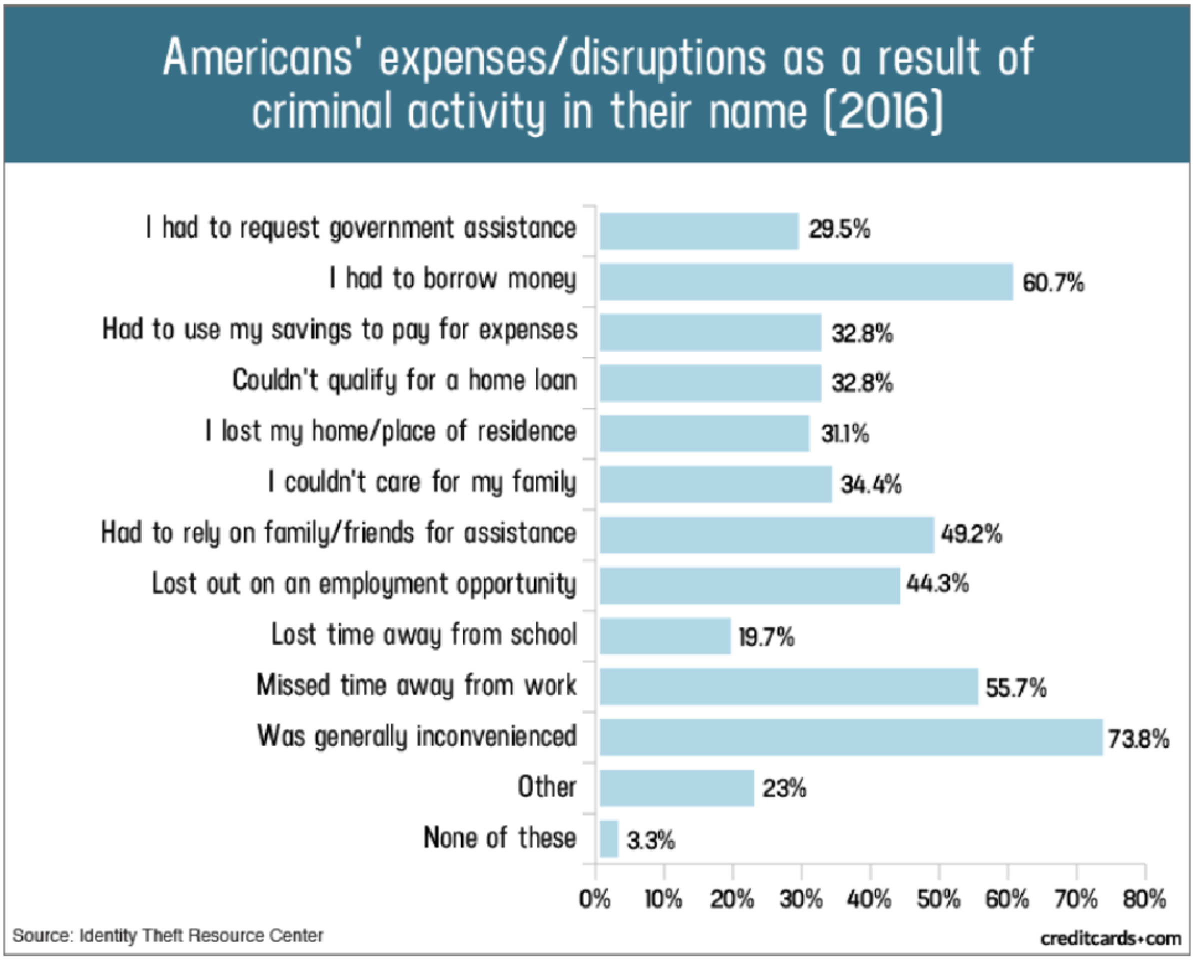
70. If, moreover, the cyber criminals also manage to steal financial information, credit and debit cards, health insurance information, driver's licenses and passports—as they did here—there is no limit to the amount of fraud that Defendant has exposed the Breach Victims to.

71. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Personal Information such as that compromised in the Data Breach:[16]

---

[15] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[16] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



72. Plaintiff and the Class have experienced one or more of these harms as a result of the Data Breach.

73. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[17]

74. Defendant's offer of two year of identity monitoring to Plaintiff and the Class is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.* fraudulent acquisition

[17] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

and use of another person's Personal Information)—it does not prevent identity theft.[18]

75. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class now have to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

76. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including Personal Information;
b. Improper disclosure of their Personal Information;
c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;
d. Damages flowing from Defendant untimely and inadequate notification of the data breach;
e. Loss of privacy suffered as a result of the data breach;
f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

[18] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost* by Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

g. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;

h. The loss of use of and access to their credit, accounts, and/or funds;

i. Damage to their credit due to fraudulent use of their Personal Information; and

j. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

77. Moreover, Plaintiff and Class have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

78. Defendant itself acknowledged the harm caused by the data breach because it offered Plaintiff and Class Members two years of identity theft repair and monitoring services. Two years of identity theft and repair and monitoring is woefully inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and Class Members for the injuries they have already suffered.

V. CLASS ALLEGATIONS

79. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

80. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a) and 23(b)(3), Plaintiff asserts all claims on behalf of a Nationwide Class, defined as follows:

> **All persons whose Personal Information was compromised by the Data Breach, including all who were sent a notice of the Data Breach.**

81. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

A. CLASS CERTIFICATION IS APPROPRIATE

82. The proposed Nationwide Class or, alternatively, the separate Statewide Classes (collectively, the "Class" as used in this sub-section) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

83. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable.

84. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant failed to adequately safeguard Plaintiff's and the Class' Personal Information;

b. Whether Defendant failed to protect Plaintiff's and the Class' Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and the Class' Personal Information violated the FTCA, state laws, and/or Defendant's other duties;

d. Whether Defendant violated the data security statutes and data breach notification statutes applicable to Plaintiff and the Class;

e. Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach expeditiously and without unreasonable delay after the Data Breach was discovered;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Breach Victims' Personal Information properly and as promised;

g. Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class' Personal Information;

h. Whether Defendant entered into implied contracts with Plaintiff and the members of the Class that included contract terms requiring Defendant to protect the confidentiality of Personal Information and have reasonable security measures;

i. Whether Defendant violated the consumer protection statutes, data breach notification statutes, and state privacy statutes applicable to Plaintiff and the Class;

j. Whether Defendant failed to notify Plaintiff and Breach Victims about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

k. Whether Defendant's conduct described herein constitutes a breach of their implied contracts with Plaintiff and the Class;

l. Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendant's wrongful conduct;

m. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Class.

85. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

86. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Class.

87. **Risks of Prosecuting Separate Actions:** This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendant are still in possession of Personal Information of Plaintiff and the Class, and Defendant's systems are still vulnerable to attack—one standard of conduct is needed to ensure the future safety of Personal Information in Defendant's possession.

88. **Policies Generally Applicable to the Class:** This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

89. **Superiority:** This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE

90. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

91. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class.

92. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiff and the Class and the importance of adequate security.

93. Defendant were well aware of the fact that hackers routinely attempted to access Personal Information without authorization. Defendant also knew about numerous, well-publicized data breaches wherein hackers stole the Personal Information from companies who held or stored such information.

94. Defendant owed duties of care to Plaintiff and the Class whose Personal Information was entrusted to it. Defendant's duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Personal Information in its possession;

b. To protect the Personal Information in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly train its employees to avoid phishing emails;

d. To use adequate email security systems, including DMARC enforcement and Sender Policy Framework enforcement, to protect against phishing emails;

e. To adequately and properly train its employees regarding how to properly and securely transmit and store Personal Information;

f. To train its employees not to store Personal Information in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

95. Because Defendant knew that a security incident, breach or intrusion upon its systems would potentially damage thousands of its current and/or former patients and employees, including Plaintiff and Class members, it had a duty to adequately protect their Personal Information.

96. Defendant owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

97. Defendant knew, or should have known, that its security practices and computer systems did not adequately safeguard the Personal Information of Plaintiff and the Class.

98. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard the Personal Information of Plaintiff and the Class.

99. Defendant breached their duties of care by failing to provide prompt notice of the Data Breach to the persons whose personal information was compromised.

100. Defendant acted with reckless disregard for the security of the Personal Information of Plaintiff and the Class because Defendant knew or should have known that their computer systems and data security practices were not adequate to safeguard the Personal Information that it collected and stored, which hackers were attempting to access.

101. Defendant acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of Personal Information compromised in the Data Breach.

102. Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class' willingness to entrust Defendant with their personal information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems (and the Personal Information stored on them) and to implement security practices to protect the Personal Information that it collected and stored from attack.

103. Defendant own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal Information. Defendant's misconduct included failing to:

a. Secure its employees' email accounts;
b. Secure access to its servers;
c. Comply with current industry standard security practices;
d. Encrypt Personal Information during transit and while stored on Defendant's systems;
e. Properly and adequately train their employees on proper data security practices;
f. Implement adequate system and event monitoring;
g. Implement the systems, policies, and procedures necessary to prevent hackers from accessing and utilizing Personal Information transmitted and/or stored by Defendant;
h. Undertake periodic audits of record-keeping processes to evaluate the safeguarding of Personal Information;
i. Develop a written records retention policy that identifies what information must be kept and for how long;
j. Destroy all discarded employee information, including information on prospective employees, temporary workers, subcontractor, and former employees;
k. Secure Personal Information and limit access to it to those with a legitimate business need;
l. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used to manage e-mail, Internet use, and so forth;
m. Avoid using Social Security numbers as a form of identification; and

n. Have a plan ready and in position to act quickly should a theft or data breach occur.

104. Defendant also had independent duties under federal and state law requiring them to reasonably safeguard Plaintiff's and the Class' Personal Information and promptly notify them about the Data Breach.

105. Defendant breached the duties they owed to Plaintiff and Class members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect their Personal Information both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards before, during, and after the period of the Data Breach; and

d. By failing to timely and accurately disclose that the Personal Information of Plaintiff and the Class had been improperly acquired or accessed in the Data Breach.

106. But for Defendant wrongful and negligent breach of the duties it owed Plaintiff and the Class members, their Personal Information either would not have been compromised or they would have been able to prevent some or all of their damages.

107. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of further harm.

108. The injury and harm that Plaintiff and Class members suffered (as alleged above) was reasonably foreseeable.

109. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

110. Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE *PER SE*

111. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

112. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiff and the Class.

113. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

114. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class as part of its business of manufacturing, selling, and installing gutter protection systems, which affects commerce.

115. Defendant violated the FTCA by failing to use reasonable measures to protect the Personal Information of Plaintiff and the Class and not complying with applicable industry standards, as described herein.

116. Defendant breached its duties to Plaintiff and the Class under the FTCA and other state data security and privacy statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Breach Victim's Personal Information.

117. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

118. Plaintiff and the Class are within the class of persons that the FTCA was intended to protect.

119. The harm that occurred as a result of the Data Breach is the type of harm the FTCA, the state data breach privacy statutes were intended to guard against.

120. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class' Personal Information.

121. Defendant breached their duties to Plaintiff and the Class by negligently and unreasonably delaying and failing to provide notice expeditiously and/or as soon as practicable to Plaintiff and the Class of the Data Breach.

122. Defendant's violation of the FTCA, state data security statutes, and/or the state data breach notification statutes constitute negligence *per se*.

123. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach by, *inter alia*, having to spend time reviewing their accounts and credit reports for unauthorized activity; spend time and incur costs to place and re-new a "freeze" on their credit; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

124. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

COUNT III – BREACH OF FIDUCIARY DUTIES

125. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged herein.

126. A relationship existed between Plaintiff and Class Members and Defendant in which Plaintiff and the Class put their trust in Defendant to protect their PII. Defendant accepted this duty and obligation when it received Plaintiff and the Class Members' PII.

127. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and refrain from disclosing their PII to unauthorized third parties.

128. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

129. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and the Class's information in Defendant's possession was adequately secured and protected.

130. Defendants also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Defendant was entrusted with Plaintiff and the Class's PII

131. Defendant breached its fiduciary duty that it owed Plaintiff and the Class by failing to case in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the PII of Plaintiff and the Class Members.

132. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiff and the Class.

133. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiff and the Class.

134. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

COUNT IV – BREACH OF CONFIDENCE

135. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

136. Defendant was fully aware of the confidential nature of the PII of Plaintiff and Class Members that it was provided.

137. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by promises and expectations that Plaintiff and Class Members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

138. Plaintiff and Class members provided their respective PII to Jersey College, and by proxy to Defendant, with the explicit and implicit understandings that Defendant would protect and not permit the PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

139. Plaintiff and Class Members provided their respective PII to Jersey College, and by proxy to Defendant, with the explicit and implicit understandings that Defendant would take precautions to protect their PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use,

and/or viewing, such as following basic principles of protecting their networks and data systems.

140. Defendant voluntarily received, in confidence, Plaintiff and Class members' PII with the understanding that the PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

141. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiff and Class Members' PII, Plaintiff and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff and Class Members' confidence, and without their express permission.

142. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages as alleged herein.

143. But for Defendant's failure to maintain and protect Plaintiff and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the misuse of Plaintiff and Class members' PII, as well as the resulting damages.

144. The injury and harm Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiff and Class members' PII. Defendant knew its data systems and protocols for accepting and securing Plaintiff and Class Members' PII had security and other vulnerabilities that placed Plaintiff and Class members' PII in jeopardy.

145. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Class Members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Plaintiff and Class Members' PII.

COUNT V – BREACH OF IMPLIED CONTRACT

146. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

147. By requiring Plaintiff and the Class Members PII to engage in or settle a litigation suit, Defendant entered into an implied contract in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff and Class Members' PII. In return, Defendant engaged in and/or settled Plaintiff and Class Members' suits.

148. Based on this implicit understanding, Plaintiff and the Class accepted Defendant's offers and provided Defendant with their PII.

149. Plaintiff and Class members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised.

150. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

151. Defendant breached the implied contracts by failing to safeguard Plaintiff and Class Members' PII.

152. Defendant also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC. These acts and omissions included (i) representing, either expressly or impliedly, that it would maintain adequate data privacy and security practices and procedures to safeguard the PII from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's PII; and (iii) failing to disclose to Plaintiffs and the Class at the time they provided their PII that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

153. The losses and damages Plaintiff and Class members sustained were the direct and proximate result of Defendant's breach of the implied contract with Plaintiff and Class Members.

COUNT VI – INVASION OF PRIVACY

154. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

155. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

156. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

157. Defendant affirmatively and recklessly disclosed Plaintiff and Class Members' PII to unauthorized third parties.

158. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII is highly offensive to a reasonable person.

159. Defendant's reckless and negligent failure to protect Plaintiff and Class Members' PII constitutes an intentional interference with Plaintiff and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

160. In failing to protect Plaintiff and Class Members' PII, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

161. Because Defendant failed to properly safeguard Plaintiff and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

162. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

163. As a proximate result of Defendant's acts and omissions, Plaintiff and the Class Members' private and sensitive PII was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

164. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

165. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff and the Class's PII.

166. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff and Class Members' PII.

167. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VII – INJUNCTIVE / DECLARATORY RELIEF

168. Plaintiff incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

169. Plaintiff and members of the Class entered into an implied contract that required Defendant to provide adequate security for the Personal Information it collected from Plaintiff and the Class.

170. Defendant owe a duty of care to Plaintiff and the members of the Class that requires them to adequately secure Personal Information.

171. Defendant still possess Personal Information regarding Plaintiff and members of the Class.

172. Since the Data Breach, Defendant has announced few if any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

173. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient information security is known to hackers, the Personal Information in Defendant possession is even more vulnerable to cyberattack.

174. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the

Class are at risk of additional or further harm due to the exposure of their Personal Information and Defendant's failure to address the security failings that lead to such exposure.

175. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

176. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
d. Ordering that Defendant's segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
e. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

f. Ordering that Defendant cease storing Personal Information in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular database scanning and securing checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

DATED: October 29, 2025

By: */s/ Catherine Ybarra*
Catherine Ybarra (Bar No. 283360)
Tyler J. Bean*
Neil P. Williams*
SIRI & GLIMSTAD LLP
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 297-3807
E: cybarra@sirillp.com
E: tbean@sirillp.com
E: nwilliams@sirillp.com

Jessica A. Wilkes*
Federman & Sherwood
10205 N. Pennsylvania Ave
Oklahoma City, OK 73120
Tel: (405) 235-1560
E: jaw@federmanlaw.com

Attorneys for Plaintiff and for the Classes

**Pro Hac Vice forthcoming*

JS-CAND 44 (Rev. 04-2025

CIVIL COVER SHEET – for people without lawyers only

See Civil Local Rule 3-2 (amended April 28, 2025), which requires the filing of a civil cover sheet only by those unrepresented by counsel.

I. PLAINTIFF(S)

JOBY CHILDRESS, individually and on behalf of all similarly situated individuals,

County of Residence of First Listed Plaintiff: Dallam County, TX
Leave blank in cases where United States is plaintiff.

Attorney or Pro Se Litigant Information *(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

DEFENDANT(S)

PROSPER FUNDING, LLC,

County of Residence of First Listed Defendant: San Fransisco, CA
Use ONLY in cases where United States is plaintiff.

Defendant's Attorney's Name and Contact Information *(if known)*

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

- [ ] U.S. Government Plaintiff
- [ ] Federal Question *(U.S. Government Not a Party)*
- [ ] U.S. Government Defendant
- [X] Diversity

III. CAUSE OF ACTION

Cite the U.S. Statute under which you are filing: *(Use jurisdictional statutes only for diversity)*
Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)

Brief description of case: Negligence due to data breach.

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

CONTRACT

- [ ] 110 Insurance
- [ ] 120 Marine
- [ ] 130 Miller Act
- [ ] 140 Negotiable Instrument
- [ ] 150 Recovery of Overpayment & Enforcement of Judgment
- [ ] 151 Medicare Act
- [ ] 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- [ ] 153 Recovery of Overpayment of Veteran's Benefits
- [ ] 160 Stockholders' Suits
- [X] 190 Other Contract
- [ ] 195 Contract Product Liability
- [ ] 196 Franchise

REAL PROPERTY

- [ ] 210 Land Condemnation
- [ ] 220 Foreclosure
- [ ] 230 Rent Lease & Ejectment
- [ ] 240 Torts to Land
- [ ] 245 Tort Product Liability
- [ ] 290 All Other Real Property

TORTS

PERSONAL INJURY

- [ ] 310 Airplane
- [ ] 315 Airplane Product Liability
- [ ] 320 Assault, Libel & Slander
- [ ] 330 Federal Employers' Liability
- [ ] 340 Marine
- [ ] 345 Marine Product Liability
- [ ] 350 Motor Vehicle
- [ ] 355 Motor Vehicle Product Liability
- [ ] 360 Other Personal Injury
- [ ] 362 Personal Injury -Medical Malpractice

PERSONAL INJURY

- [ ] 365 Personal Injury – Product Liability
- [ ] 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- [ ] 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY

- [ ] 370 Other Fraud
- [ ] 371 Truth in Lending
- [ ] 380 Other Personal Property Damage
- [ ] 385 Property Damage Product Liability

CIVIL RIGHTS

- [ ] 440 Other Civil Rights
- [ ] 441 Voting
- [ ] 442 Employment
- [ ] 443 Housing/ Accommodations
- [ ] 445 Amer. w/Disabilities–Employment
- [ ] 446 Amer. w/Disabilities–Other
- [ ] 448 Education

PRISONER PETITIONS

HABEAS CORPUS

- [ ] 463 Alien Detainee
- [ ] 510 Motions to Vacate Sentence
- [ ] 530 General
- [ ] 535 Death Penalty

OTHER

- [ ] 540 Mandamus & Other
- [ ] 550 Civil Rights
- [ ] 555 Prison Condition
- [ ] 560 Civil Detainee– Conditions of Confinement

FORFEITURE/PENALTY

- [ ] 625 Drug Related Seizure of Property 21 USC § 881
- [ ] 690 Other

LABOR

- [ ] 710 Fair Labor Standards Act
- [ ] 720 Labor/Management Relations
- [ ] 740 Railway Labor Act
- [ ] 751 Family and Medical Leave Act
- [ ] 790 Other Labor Litigation
- [ ] 791 Employee Retirement Income Security Act

IMMIGRATION

- [ ] 462 Naturalization Application
- [ ] 465 Other Immigration Actions

BANKRUPTCY

- [ ] 422 Appeal 28 USC § 158
- [ ] 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS

- [ ] 820 Copyrights
- [ ] 830 Patent
- [ ] 835 Patent—Abbreviated New Drug Application
- [ ] 840 Trademark
- [ ] 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY

- [ ] 861 HIA (1395ff)
- [ ] 862 Black Lung (923)
- [ ] 863 DIWC/DIWW (405(g))
- [ ] 864 SSID Title XVI
- [ ] 865 RSI (405(g))

FEDERAL TAX SUITS

- [ ] 870 Taxes (U.S. Plaintiff or Defendant)
- [ ] 871 IRS–Third Party 26 U.S.C. § 7609

OTHER STATUTES

- [ ] 375 False Claims Act
- [ ] 376 Qui Tam (31 USC § 3729(a))
- [ ] 400 State Reapportionment
- [ ] 410 Antitrust
- [ ] 430 Banks and Banking
- [ ] 450 Commerce
- [ ] 460 Deportation
- [ ] 470 Racketeer Influenced & Corrupt Organizations
- [ ] 480 Consumer Credit
- [ ] 485 Telephone Consumer Protection Act
- [ ] 490 Cable/Sat TV
- [ ] 850 Securities/Commodities/ Exchange
- [ ] 890 Other Statutory Actions
- [ ] 891 Agricultural Acts
- [ ] 893 Environmental Matters
- [ ] 895 Freedom of Information Act
- [ ] 896 Arbitration
- [ ] 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- [ ] 950 Constitutionality of State Statutes

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

- [X] Original Proceeding
- [ ] Removed from State Court
- [ ] Remanded from Appellate Court
- [ ] Reinstated or Reopened
- [ ] Transferred from Another District
- [ ] Multidistrict Litigation–Transfer
- [ ] Multidistrict Litigation–Direct File

VI. FOR DIVERSITY CASES ONLY: CITIZENSHIP OF PRINCIPAL PARTIES

(Place an "X" in One Box for Plaintiff and One Box for Defendant)

Plaintiff	Defendant	
[ ]	[ ]	Citizen of California
[X]	[ ]	Citizen of Another State
[ ]	[ ]	Citizen or Subject of a Foreign Country
[ ]	[X]	Incorporated or Principal Place of Business In California
[ ]	[ ]	Incorporated and Principal Place of Business In Another State
[ ]	[ ]	Foreign Nation

VII. REQUESTED IN COMPLAINT

- [X] Check if the complaint contains a **jury demand.**
- [X] Check if the complaint contains a **monetary demand**. Amount: 1,000,000.00
- [X] Check if the complaint seeks **class action** status under Fed. R. Civ. P. 23.
- [ ] Check if the complaint seeks a **nationwide injunction** or Administrative Procedure Act vacatur.

VIII. RELATED CASE(S) OR MDL CASE

Provide case name(s), number(s), and presiding judge(s).

3:25-cv-07947-CRB McPhee v. Prosper Funding, LLC; 3:25-cv-07949-CRB Walston v. Prosper Funding, LLC; 3:25-cv-08177-CRB
3:25-cv-08232-CRB; 3:25-cv-08634-CRB
3:25-cv-07958-CRB Chavira et al v. Prosper Funding, LLC; 3:25-cv-07972-CRB YODER v. PROSPER FUNDING LLC;
3:25-cv-07977-CRB Park v. Prosper Funding LLC et al; 3:25-cv-08169-CRB Valencia v. Prosper Funding, LLC

IX. DIVISIONAL ASSIGNMENT pursuant to Civil Local Rule 3-2

(Place an "X" in One Box Only)

- [X] **SAN FRANCISCO/OAKLAND**
- [ ] **SAN JOSE**
- [ ] **EUREKA-MCKINLEYVILLE**

DATE 10/29/2025 **SIGNATURE OF ATTORNEY OR PRO SE LITIGANT** */s/ Catherine Ybarra*

COMPLETING THE CIVIL COVER SHEET

Complete the form as follows:

I. Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.

Attorney/Pro Se Litigant Information. Enter the firm name, address, telephone number, and email for attorney of record or pro se litigant. If there are several individuals, list them on an attachment.

II. Jurisdiction. Under Federal Rule of Civil Procedure 8(a), pleadings must establish the basis of jurisdiction. If multiple bases for jurisdiction apply, prioritize them in the order listed:

(1) *United States plaintiff*. Jurisdiction based on 28 U.S.C. §§ 1345 and 1348 for suits filed by the United States, its agencies or officers.

(2) *United States defendant.* Applies when the United States, its agencies, or officers are defendants.

(3) *Federal question*. Select this option when jurisdiction is based on 28 U.S.C. § 1331 for cases involving the U.S. Constitution, its amendments, federal laws, or treaties (but use choices 1 or 2 if the United States is a party).

(4) *Diversity of citizenship.* Select this option when jurisdiction is based on 28 U.S.C. § 1332 for cases between citizens of different states and complete Section VI to specify the parties' citizenship. Note: Federal question jurisdiction takes precedence over diversity jurisdiction.

III. Cause of Action. Enter the statute directly related to the cause of action and give a brief description of the cause. Do not cite jurisdictional statutes unless jurisdiction is based on diversity. Example: U.S. Civil Statute: 47 U.S.C. § 553. Brief Description: Unauthorized reception of cable service.

IV. Nature of Suit. Check one of the boxes. If the case fits more than one nature of suit, select the most definitive or predominant.

V. Origin. Check one of the boxes:

(1) *Original Proceedings*. Cases originating in the United States district courts.

(2) *Removed from State Court*. Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C. § 1441. When the petition for removal is granted, check this box.

(3) *Remanded from Appellate Court*. Check this box for cases remanded to the district court for further action, using the date of remand as the filing date.

(4) *Reinstated or Reopened*. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) *Transferred from Another District*. Check this box for cases transferred under Title 28 U.S.C. § 1404(a). Do not use this for within-district transfers or multidistrict litigation (MDL) transfers.

(6) *Multidistrict Litigation Transfer*. Check this box when a multidistrict (MDL) case is transferred into the district under authority of Title 28 U.S.C. § 1407.

(7) *Multidistrict Litigation Direct File.* Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

VI. Residence (citizenship) of Principal Parties. Mark for each principal party *only* if jurisdiction is based on diversity of citizenship.

VII. Requested in Complaint.

(1) *Jury demand.* Check this box if plaintiff's complaint demanded a jury trial.

(2) *Monetary demand*. For cases demanding monetary relief, check this box and enter the actual dollar amount being demanded.

(3) *Class action.* Check this box if plaintiff is filing a class action under Federal Rule of Civil Procedure 23.

(4) *Nationwide injunction.* Check this box if plaintiff is seeking a nationwide injunction or nationwide vacatur pursuant to the Administrative Procedures Act.

VIII. Related Cases. If there are related pending case(s), provide the case name(s) and number(s) and the name(s) of the presiding judge(s). If a short-form MDL complaint is being filed, furnish the MDL case name and number.

IX. Divisional Assignment. Identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated." Note that case assignment is made without regard for division in the following case types: Property Rights (Patent, Trademark and Copyright), Prisoner Petitions, Securities Class Actions, Anti-Trust, Bankruptcy, Social Security, and Tax.