

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

RANDY HARRIS individually and on
behalf of all others similarly situated,

Plaintiff,

v.

ONEMAIN FINANCIAL GROUP, LLC,

1501 S Clinton St., Suite 600, Baltimore,
Maryland, 21224,
Baltimore County, Maryland

Defendant.

Case No.:

COMPLAINT – CLASS ACTION

JURY TRIAL DEMANDED

Plaintiff Randy Harris (“Plaintiff”), individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against OneMain Financial Group, LLC (“Defendant”). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information (“PII”¹ or “Private Information”) and that was impacted in a data breach (the “Data Breach” or the “Breach”).

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is a consumer finance company that specializes in offering secured and unsecured personal installment loans to borrowers with below-average or fair-to-bad credit.

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Defendant experienced a Data Breach that resulted in the exposure of highly sensitive Private Information, including names, addresses, and Social Security numbers.²

6. On September 25, 2026, Defendant filed a notice of public disclosure about the Data Breach.³

7. Defendant failed to take precautions designed to keep individuals' Private Information secure.

8. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

9. Armed with the Private Information accessed in the Data Breach (and a head start),

² *Data Breach Security Reports*, OneMain Financial Group, LLC, Office of the Texas Attorney General: <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage> (last visited Sept. 28, 2026).

³ *Id.*

data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

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

11. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to affected individuals such as Plaintiff and Class Members, of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

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

13. Upon information and belief, Defendant failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Defendant properly monitored its IT Network, it would have discovered the Breach sooner.

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

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.

PARTIES

Plaintiff

16. Plaintiff is a citizen and resident of Loves Park, Illinois.

Defendant

17. Defendant is a limited liability company maintaining its principal place of business at 1501 S Clinton St., Suite 600, Baltimore, Maryland, 21224. Defendant's registered agent is The Corporation Trust Incorporated located at 2405 York Rd, Suite 201, Lutherville-Timonium, Maryland, 21093.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d) (2) (A). Defendant has its principal place of business located in this District.

19. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in this District.

20. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

21. Defendant is a consumer finance company that specializes in offering secured and unsecured personal installment loans to borrowers with below-average or fair-to-bad credit.

22. As a condition of providing services, Defendant requires that individuals entrust it with highly sensitive personal information.

23. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

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

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

B. The Data Breach

26. Defendant experienced a Data Breach that resulted in the exposure of highly

sensitive Private Information, including names, addresses, and Social Security numbers.⁴

27. On September 25, 2026, Defendant filed a notice of public disclosure about the Data Breach.⁵

28. Defendant had obligations created by the FTC Act, contract, common law, and industry standards to keep Plaintiff and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

30. The Data Breach resulted in unauthorized third-party accessing and acquiring files containing unencrypted Private Information of Plaintiff and Class Members. Plaintiff and Class Members' Private Information was accessed and stolen in the Data Breach.

31. Upon information and belief, Plaintiff's Private Information, and that of Class Members, was subsequently published on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

32. Defendant failed to take precautions designed to keep individuals' Private Information secure.

33. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

⁴ *Data Breach Security Reports*, OneMain Financial Group, LLC, Office of the Texas Attorney General: <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage> (last visited Sept. 28, 2026).

⁵ *Id.*

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

34. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

35. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

36. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,⁶ Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present customers Private Information.

37. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.⁷ Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

D. The Harm Caused by the Data Breach Now and Going Forward

38. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open

⁶ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>

⁷ *Id.*

new utility accounts, or get medical treatment on your health insurance.”⁸

39. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

40. Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

41. Stolen Private Information is often trafficked on the “dark web,” a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the “dark web” due to this encryption, which allows users and criminals to conceal their identities and online activity.

42. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.⁹

43. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online “dark market”—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person’s identity.”¹⁰ Marketplaces similar to the now-defunct AlphaBay continue to be “awash with [PII] belonging to victims from countries all over the world.”¹¹

44. PII remains of high value to criminals, as evidenced by the prices they will pay

⁸ *Prevention and Preparedness*, New York State Police, <https://troopers.ny.gov/prevention-and-preparedness>

⁹ *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) <https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring>

¹⁰ *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), <https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/>

¹¹ *Id.*

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 \$200.¹² Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹³

45. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than \$3.5 billion in losses to individuals and business victims.¹⁴

46. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."¹⁵ Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen.

47. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or

¹² *Id.*

¹³ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) <https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>

¹⁴ *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion>

¹⁵ *Id.*

potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' Private Information.

48. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

49. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

50. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative

acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

Plaintiff's Experience and Injuries

51. Plaintiff is a customer of Defendant.

52. As a condition of obtaining services, Plaintiff was required to provide Defendant with his Private Information.

53. Defendant was in possession of Plaintiff's Private Information before, during and after the Data Breach.

54. Plaintiff reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

55. Plaintiff greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

56. Plaintiff stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information

or that may contain any information that could otherwise be used to compromise his identity and credit card accounts.

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

58. As a result of the Data Breach, Plaintiff has spent several hours researching the Data Breach, reviewing his bank accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff would have spent on other activities, including but not limited to work and/or recreation.

59. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing him of the fact that his Private Information was acquired by criminals as a result of the Data Breach.

60. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

61. Plaintiff has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

62. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now

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

CLASS ALLEGATIONS

63. Plaintiff brings this class action, individually and on behalf of the following classes:

Nationwide Class: All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach (the “Nationwide Class”).

64. Specifically excluded from the Classes are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge’s immediate family.

65. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

66. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

67. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates

that the Class is comprised of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

68. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

69. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

70. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

71. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

- a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- b. Whether Defendant's data security systems prior to and during the Data

Breach complied with applicable data security laws and regulations;

- c. Whether Defendant's storage of Plaintiff and Class Member's Private Information was done in a negligent manner;
- d. Whether Defendant had a duty to protect and safeguard Plaintiff and Class Members' Private Information;
- e. Whether Defendant's conduct was negligent;
- f. Whether Defendant's conduct violated Plaintiff and Class Members' privacy;
- g. Whether Defendant took sufficient steps to individuals' Private Information;
- h. Whether Defendant was unjustly enriched; and
- i. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

72. Information concerning Defendant's policies is available from Defendant's records.

73. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

74. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

75. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

76. Plaintiff restates and realleges all of the allegations contained in paragraphs 1-75,

as if fully set forth herein.

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

78. Defendant's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

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

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

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. To protect the Private Information in its possession it using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

- e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

81. Defendant's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

82. Defendant's duty also arose because Defendant was bound by industry standards to protect the confidential Private Information entrusted to it.

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

84. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class Members' Private Information within Defendant's possession.

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

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

87. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff and Class Members' Private Information. The specific negligent acts

and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to comply with the FTCA;
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

88. Defendant acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

89. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff and Class Members' willingness to entrust Defendant with their Private 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 Private Information that it stored on them) from attack.

90. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

91. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members

regarding the Data Breach, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

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

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

94. Defendant also had independent duties under state laws that required it to reasonably safeguard Plaintiff and Class Members' Private Information and promptly notify them about the Data Breach.

95. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

96. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

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

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

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class)

99. Plaintiff restates and realleges all of the allegations contained in paragraphs 1-75, as if fully set forth herein.

100. Pursuant to Section 5 of the FTCA, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

101. Defendant breached its duties to Plaintiff and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

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

103. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendant's duty in this regard.

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

105. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff and Class Members' Private Information in compliance with applicable laws would result in an unauthorized

third-party gaining access to Defendant's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

106. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect and Defendant's failure to comply with both constitutes negligence *per se*.

107. Plaintiff and Class Members' Private Information constitutes personal property that was stolen due to Defendant's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

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

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

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

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

111. Plaintiff restates and realleges all of the allegations contained in paragraphs 1-75, as if fully set forth herein.

112. Plaintiff and Class Members were required to provide their PII to Defendants as a condition of receiving services from Defendants. Plaintiff and Class Members provided their PII to Defendants in exchange for Defendant's services.

113. Plaintiff and Class Members (or their third-party agents) reasonably understood that a portion of the funds paid for services would be used to pay for adequate cybersecurity measures.

114. Plaintiff and Class Members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants duties under state and federal law, and their internal policies.

115. Plaintiff and the Class Members accepted Defendants' offers by disclosing their PII to Defendants in exchange for services.

116. In turn, and through internal policies, Defendants agreed to protect and not disclose the PII to unauthorized persons.

117. On information and belief, Defendants maintain internal policies that represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

118. Implicit in the parties' agreement was that Defendants would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

119. After all, Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of such an agreement with Defendants.

120. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

121. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain.

In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

122. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

123. Defendant materially breached the contracts they entered with Plaintiff and Class members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendants created, received, maintained, and transmitted.

124. In these and other ways, Defendants violated their duty of good faith and fair dealing.

125. Defendant's breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

126. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the internet and/or the Dark Web.

127. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendants conduct.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

128. Plaintiff restates and realleges all of the allegations contained in paragraphs 1-75, as if fully set forth herein.

129. Plaintiff and Class Members conferred a benefit on Defendant by turning over their Private Information to Defendant. Moreover, upon information and belief, Plaintiff alleges that monies received by Defendant included payment for cybersecurity protection to protect Plaintiff and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiff and Class Members in the form of elevated prices charged by Defendant for their services. Plaintiff and Class Members did not receive such protection.

130. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiff and Class Members.

131. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

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

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

134. If Plaintiff and Class Members had known that Defendant had not adequately

secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

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

136. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) 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; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

or compensation.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seek the following relief:

- 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 is a proper representative of the Nationwide Class requested herein;
- b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;
- e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs,

and expenses as allowable by law; and

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 28, 2026,

Respectfully submitted,

By: /s/ Mariya Weekes

Mariya Weekes (USDC MD Bar No. 32052)

MILBERG, PLLC

333 SE 2nd Avenue,

Suite 2000

Miami, FL, 33131

Tel: (786) 206-9057

mweekes@milberg.com

Attorney for Plaintiff and the Proposed Class