UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

JOY DRYER, *on behalf of herself and all others similarly situated*, *Plaintiff*, **v.** NATIONWIDE RETIREMENT SOLUTIONS, INC., *Defendant.*	)	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Joy Dryer ("Plaintiff"), individually and on behalf of all others similarly situated, by and through counsel, brings this Class Action Complaint ("Complaint") against Defendant Nationwide Retirement Solutions, Inc., and based upon personal knowledge with respect to herself, and on information and belief and the investigation of counsel as to all other matters, in support thereof alleges as follows:

NATURE OF THE ACTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Nationwide Retirement Solutions, Inc., arising from its failure to safeguard certain Personally Identifying Information[1] ("PII") and other sensitive, non-public financial information (collectively, "Personal Information") of thousands of its prospective, current, and

[1] The Federal Trade Commission defines "personally identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the breach.

former customers, resulting in Defendant's systems being unauthorizedly accessed and the Personal Information of customers therein, including of Plaintiff and the proposed Class Members, being disclosed, stolen, compromised, and misused, causing widespread and continuing injury and damages.

2. On information and belief, for an unknown period of time until at least September 3, 2022, Nationwide's systems were "hacked" and unauthorizedly accessed, resulting in the unauthorized disclosure of the Personal Information of Plaintiff and the Class Members, including names, Social Security Numbers,[2] PII, and financial account information and numbers (the "Data Breach").[3]

3. On information and belief, over 1,600 persons were impacted by the Data Breach.[4]

4. As explained below, Plaintiff and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by Nationwide, and the resulting misuse of their Personal Information and fraudulent activity, including fraudulent attempts to open bank accounts, decreased credit scores, monetary damages including out-of-pocket expenses, including those associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiff and the Class also now forever face an amplified risk of *further* misuse, fraud, and identity theft due to their sensitive Personal Information falling into the hands of cybercriminals as a result of the tortious conduct of Defendant.

---

[2] *See:* Nationwide sample Notice of Data Breach to Montana and Massachusetts Attorneys General, available at https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-550.pdf; https://www.mass.gov/doc/assigned-data-beach-number-28339-nationwide-retirement-solutions-inc/download (last accessed October 14, 2022).

[3] *Id.*

[4] Nationwide report to Maine Attorney General, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/bc089c64-8385-4b4e-8811-07a9c6932a92.shtml (last accessed October 14, 2022).

5. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action for negligence, negligence *per se*, breach of express and implied contractual duties, unjust enrichment, and invasion of privacy. Plaintiff seeks damages and injunctive and declaratory relief arising from Nationwide's failure to adequately protect her highly sensitive Personal Information.

PARTIES

6. Plaintiff, Joy Dryer, is a natural person and citizen of North Carolina, residing in Asheville, North Carolina, where she intends to remain. Plaintiff is a Nationwide customer and Data Breach victim, who received Nationwide's Breach Notice on or around September 13, 2022.

7. Defendant, Nationwide Retirement Solutions, Inc., is a Delaware corporation with its principal place of business in Columbus, Ohio. Its headquarters are located at One Nationwide Plaza, Columbus, Ohio, 43215. In addition, the majority of Nationwide's officers direct, control, and coordinate its corporate activities from that same location – One Nationwide Plaza, Columbus, Ohio, 43215. Thus, Nationwide is a citizen of Ohio.

8. Defendant Nationwide Retirement Solutions, Inc. is an affiliate company of the insurance and financial services provider, Nationwide Mutual Insurance Company.

9. Nationwide Retirement Solutions Inc. ("Nationwide") seeks to provide retirement, investment, and insurance services.

JURISDICTION & VENUE

10. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which at least one member of the class (Ms. Dryer) is a citizen of a State different from the Defendant. The number of members of the proposed Class in aggregate exceeds 100 consumers. 28 U.S.C. § 1332(d)(5)(B).

11. This Court has personal jurisdiction over Nationwide because Nationwide is headquartered and regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and/or services provided to persons in this District and in Ohio.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(d) because the Defendant is a corporation that resides in this District.

FACTUAL ALLEGATIONS

A. Plaintiff and the Class Members entrusted their Personal Information to Nationwide

13. Plaintiff Dryer and the Class Members are present and prospective customers of Nationwide.

14. Plaintiff Dryer has been enrolled in a retirement plan with Nationwide for the past 25 years.

15. As a condition of enrolling in a retirement plan with Nationwide, Plaintiff and the Class Members were required by Nationwide to confide and make available to their it their sensitive confidential Personal Information.

16. In exchange, Nationwide promises to secure its customers' PII as part of their agreements for retirement benefits.

17. Indeed, Nationwide represents it has duties to safeguard its customers' PII in its privacy policies.

18. Nationwide states that it collects its customers' information for "product servicing or marketing purposes" and that "access [to its customers' personal information] is limited to those who require your information to do their jobs." [5]

[5] *See* Nationwide's Privacy and Security Policy (attached as **Exhibit A**).

19. The types of personal information that Nationwide collects includes: name, phone number, contact information, social security number, assets and income, account and/or policy information, driver's license number, financial information, consumer report information, application and transaction information, public records, and family or beneficiary information. [6]

20. Nationwide also states that medical information "may also need to be collected" although it is "not shared for marketing purposes[.]"[7]

21. Nationwide states that personal information "may be collected" when customers:

- Create an online account
- Access your account/policy online
- Apply for products or services
- Send information online/via email
- Complete a form
- Subscribe to an email list
- Apply for a job
- Complete an online transaction
- Use tools & calculators
- Complete and online survey.[8]

22. Nationwide acknowledges the value of protecting its customers' personal information. In its company Privacy and Security Policy, Nationwide promises that "[p]hysical and technical means are used to ensure the security and confidentiality of [its customers]

[6] *See* **Exhibit A.**
[7] *Id*.
[8] *Id*.

information."[9]

23. Nationwide states in its Privacy and Security Policy that it complies with state and federal laws regarding data security and data breach notifications, which it violated by failing to implement and enforce reasonable cybersecurity measures.

24. Nationwide also promises to delete data when it no longer needs it:

> We retain your information in accordance with our legal obligations and records retention policies. For example, we may have a legal obligation to retain information relating to your agreements with us or claims relating to your products or services. We delete your data once the legal obligation expires or after the period of time specified in our records retention policies.[10]

25. In its Privacy and Security Policy, Nationwide promises that it will not sell Personal Information to third parties for business or commercial purposes, but does indicate that Personal Information may be kept or tracked by business partners "in the process of developing and servicing [Nationwide's] websites."

26. But, on information and belief, Nationwide never implemented or enforced the reasonable cybersecurity measures and policies necessary to deliver on those promises.

27. The Data Breach that is the subject of this civil action is not contemplated or permitted by Nationwide's website Privacy Policy.

28. Plaintiff and the proposed Class Members entrusted their Personal Information to Nationwide solely for the purposes of applying for retirement benefits with Defendant and/or as a condition of signing up for a retirement plan, with the expectation and implied mutual understanding that Nationwide would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

29. Plaintiff and the proposed Class Members would not have entrusted Nationwide

[9] *Id.*
[10] *Id.*

with their highly sensitive Personal Information if they had known that Nationwide would fail to take adequate measures to protect it from unauthorized use or disclosure.

B. Plaintiff's and the Class Members' Personal Information was Unauthorizedly Disclosed and Compromised in the Data Breach

30. Plaintiff Dryer has been enrolled in a Nationwide retirement plan for the past 25 years.

31. As a prerequisite to enrolling in a retirement plan, Plaintiff and the Class Members disclosed their non-public and sensitive Personal Information to Nationwide with the implicit understanding that their Personal Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their enrollment, and the express, specific, written representations made by Nationwide and its agents.

32. Plaintiff and the Class Members reasonably relied upon Nationwide's representations to their detriment and would not have provided their sensitive Personal Information to Nationwide if not for Nationwide's explicit and implicit promises to adequately safeguard that information.

33. From an unknown date until at least September 3, 2022, hackers bypassed Nationwide's cybersecurity undetected and accessed its customers' PII. Nationwide did not detect the hack when it happened, meaning Nationwide did not have the means to prevent, detect, or stop data breaches before hackers could access and steal PII.

34. On September 12, 2022, Nationwide began sending letters to the Class Members notifying them that their Personal Information had been compromised during the Data Breach ("Notice"). Dryer received the Notice on or around September 13, 2022.

35. According to Nationwide's Notice, on or around September 3, 2022, Nationwide "received an email from an anonymous source claiming to have acquired certain personal

information about [its customers]." *Id*. Nationwide told its customers that Nationwide "confirmed that your information, which we maintain to service your current or past retirement plan, was included in the information acquired by an unauthorized party." *Id.*

36. Through its investigation, Nationwide determined that an unauthorized actor may have accessed and obtained this sensitive information

37. The information that was exposed in the Data Breach included Plaintiff and the Class Members' "date of birth, email and physical address, gender, full name, phone number, and Social Security Number." *Id.*

38. Nationwide stated that it notified regulators, plan sponsors, impacted individuals, and law enforcement about the breach. Nationwide offered those affected by the Data Breach two years of credit monitoring and identity theft protection through Equifax Complete Premier.

39. Criminals could steal customers' information because Nationwide never implemented the cybersecurity measures necessary to protect it, leaving that information an unguarded target for theft and misuse.

40. Thus, cybercriminals accessed and stole customers' PII, including their names and Social Security numbers, date of birth, email and physical address, gender, and phone number.

41. As a result of this Data Breach, the Personal Information of Plaintiff and the proposed Class Members, believed to be over 1,600 individuals, was unauthorizedly disclosed and compromised in the Data Breach.

42. The Data Breach was preventable and a direct result of Nationwide's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' Personal Information.

C. Plaintiff's Experience

43. Plaintiff has been affiliated with Nationwide as a retirement plan customer for over

25 years.

44. Plaintiff provided her Personal Information to Nationwide and trusted that the company would use reasonable measures to protect it according to Nationwide's internal policies and state and federal law.

45. Following the Data Breach, on or around September 19, 2022, Plaintiff suffered identity theft when her credit card was fraudulently charged without her permission.

46. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

D. Defendant failed to adhere to FTC guidelines.

47. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

48. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

49. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

E. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

53. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

54. The Personal Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach— most

notably names and Social Security Numbers —is difficult, if not impossible, to change.

55. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[11]

56. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining PII with false provider numbers to file fake claims with insurers.

57. The value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

58. As a result of Nationwide's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

f. The loss of the opportunity to control how their PII is used;

g. The diminution in value of their PII;

h. The compromise and continuing publication of their PII;

i. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

[11] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

j. Lost opportunity costs and lost wages associated with the time and effort expended 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 and fraud;

k. Delay in receipt of tax refund monies;

l. Unauthorized use of stolen PII; and

m. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

59. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

60. The value of Plaintiff and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

61. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

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

63. 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.

64. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's 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. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

65. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

66. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

67. Plaintiff sues on behalf of themself and the proposed Class ("Class"), defined as follows:

> All individuals whose PII was compromised as a result of Nationwide's Data Breach which occurred in or around September 2022.

68. Excluded from the Class are Nationwide and its subsidiaries and affiliates, officers, directors, and members of their immediate families, and any entity in which it has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

69. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or to add a subclass(es) if necessary, before this Court determines whether certification is appropriate.

70. *Fed. R. Civ. Proc. 23(a)(1) Numerosity:* The Class is so numerous such that joinder of all Members is impracticable. Upon information and belief, and subject to class discovery, the Class consists of more than 1,600 customers of Nationwide, the identity of whom are within the exclusive knowledge of and can be ascertained only by resort to Nationwide's records. Nationwide has the administrative capability through its computer systems and other records to identify all Members of the Class, and such specific information is not otherwise available to Plaintiff.

71. *Fed. R. Civ. Proc. 23(a)(2) Commonality and Fed. R. Civ. Proc. 23(b)(3) Predominance:* There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Members of the Class because Nationwide has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Nationwide had a duty to protect customer Personal Information;

b. Whether Nationwide knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Nationwide's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether Nationwide was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Nationwide's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether Nationwide's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unlawful exposure of the Plaintiff's and Class Members' Personal Information;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Nationwide's failure to reasonably protect its systems and data network;

h. Whether Plaintiff and Class Members are entitled to relief;

i. Whether Nationwide failed to adequately notify Class Members of the compromise of their Personal Information;

j. Whether Nationwide assumed a fiduciary duty and/or confidential relationship to Class Members when they entrusted it with their Personal Information;

k. Whether Nationwide breached its contracts with Class Members by failing to properly safeguard their Personal Information;

l. Whether Nationwide's violation of FTC regulations constitutes evidence of negligence or negligence *per se*;

m. Whether Nationwide impliedly warranted to Class Members that the information technology systems were fit for the purpose intended, namely the safe and secure

processing of Personal Information, and whether such warranty was breached.

72. *Fed. R. Civ. Proc. 23(a)(3) Typicality:* Plaintiff's claims are typical of the claims of all Class Members, because all such claims arise from the same set of facts regarding Nationwide's failures:

a. to protect Plaintiff's and Class Members' Personal Information;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiff and Class Members in a complete and timely manner information concerning the security breach and the theft of their Personal Information.

73. *Fed. R. Civ. Proc. 23(a)(4) Adequacy:* Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff is a more than adequate representative of the Class in that Plaintiff is a victim of the Data Breach, has suffered injury and damages such as misuse and fraudulent activity as a result of the Data Breach, and brings the same claims on behalf of herself and the putative Class. Plaintiff has no interests antagonistic to that of the Class Members. Plaintiff has retained counsel who are competent and experienced in litigating class actions, including class actions following data breaches and unauthorized data disclosures. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

74. *Fed. R. Civ. Proc. 23(b)(2) Injunctive and Declaratory Relief:* Nationwide has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

75. *Fed. R. Civ. Proc. 23(b)(3) Superiority:* It is impracticable to bring Class Members' individual claims before the Court. Class treatment permits many similarly situated persons to

prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

76. A class action is superior to the other available methods for the fair and efficient adjudication of this controversy because:

77. The unnamed Members of the Class are unlikely to have an interest in individually controlling the prosecution of separate actions;

78. Concentrating the litigation of the claims in one forum is desirable;

79. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

80. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

81. Plaintiff knows of no unique difficulty to be encountered in the prosecution of this action that would preclude its maintenance as a class action.

82. *Fed. R. Civ. Proc. 23(c)(4) Issue Certification:* Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

83. Whether Nationwide owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their Personal Information;

84. Whether Nationwide's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

85. Whether Nationwide's failure to institute adequate protective security measures amounted to negligence;

86. Whether Nationwide failed to take commercially reasonable steps to safeguard current and prospective customers' Personal Information; and

87. Whether adherence to FTC data security recommendations, and industry standards on data security would have reasonably prevented the Data Breach.

88. Finally, all Members of the proposed Class are readily ascertainable. Nationwide has access to customer and applicant names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing constitutionally sufficient notice.

COUNT I
NEGLIGENCE

89. Plaintiff Dryer and the Members of the Class incorporate the above allegations as if fully set forth herein.

90. Defendant Nationwide owed a duty to Plaintiff and the Members of the Class to exercise reasonable care to safeguard their Personal Information in its possession, based on the foreseeable risk of a data breach and the resulting exposure of their information, as well as on account of the special relationship between Defendant and its customers, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

91. Defendant acted with wanton and reckless disregard for the security and

confidentiality of Plaintiff's and Members of the Class's Personal Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

92. Further, Defendant owed to Plaintiff and Members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Personal Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Members of the Class to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

93. Nationwide owed these duties to Plaintiff and Members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Members of the Class's personal information and PII for purposes of selling retirement plans.

94. Plaintiff and Members of the Class were required to provide their Personal Information to Defendant as a condition of applying for retirement benefits, and Defendant retained that information.

95. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable. Given that Defendant holds vast amounts of this sensitive information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Personal Information, whether by email hacking attack, or

otherwise.

96. Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Members of the Class, and the importance of exercising reasonable care in handling it.

97. Defendant Nationwide breached its duties by failing to exercise reasonable care in supervising its employees and agents, and in handling and securing the Personal Information and PII of Plaintiff and Members of the Class which actually and proximately caused the Data Breach and Plaintiff's and Members of the Class's injury.

98. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Members of the Class have suffered or will suffer injury and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

99. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face

COUNT II
NEGLIGENCE *PER SE*

100. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

101. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' Personal Information, PII.

102. Section 5 of the FTC Act 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 customers or, in this case, current and prospective customers' PII.

103. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

104. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its current and prospective customers' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had required and solicited, collected, and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to customers in the event of a breach, which ultimately came to pass.

105. The harm that has occurred in the Data Breach is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

106. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard their PII.

107. Defendant breached its respective duties to Plaintiff and Members of the Class

under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' PII.

108. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

109. But-for Nationwide's wrongful and negligent breach of its duties owed to Plaintiff and the Class, Plaintiff and the Members of the Class would not have been injured.

110. The injury and harm suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and Members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

111. Had Plaintiff and Members of the Class known that Defendant did not adequately protect current and prospective customers' PII, Plaintiff and Members of the Class would not have entrusted Defendant with their PII.

112. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered harm, injury, and damages as set forth in the preceding paragraphs.

COUNT III
BREACH OF EXPRESS/IMPLIED CONTRACTUAL DUTY

113. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

114. Defendant offered to provide retirement plans to Plaintiff and Members of the Class in exchange for payment.

115. Nationwide also required Plaintiff and the Members of the Class to provide Defendant with their Personal Information as a condition of applying for retirement benefits.

116. In turn, and through its Privacy Policy, Defendant agreed it would not disclose

Personal Information it collects to unauthorized persons. Defendant also promised to maintain safeguards to protect their Personal Information.

117. Plaintiff and the Members of the Class accepted Defendant's offer by providing Personal Information to Nationwide, in applying for retirement plans.

118. The agreement was supported by adequate consideration, as it was an exchange of labor for money.

119. Implicit in the Parties' agreement was that Defendant would provide Plaintiff and Members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Personal Information.

120. Plaintiff and the Members of the Class would not have entrusted their Personal Information to Defendant in the absence of such agreement with Defendant.

121. Nationwide materially breached the contract(s) it had entered with Plaintiff and Members of the Class by failing to safeguard such Personal Information. Defendant further breached the implied contracts with Plaintiff and Members of the Class by:

a. Failing to properly safeguard and protect Plaintiff' and Members of the Class's Personal Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic Personal Information that Defendant received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

122. The damages sustained by Plaintiff and Members of the Class as set forth in the preceding paragraphs were the direct and proximate result of Defendant's material breaches of its

agreement(s).

123. Plaintiff and Members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

124. The covenant of good faith and fair dealing is implied into every contract. The 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—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

126. In these and other ways, Defendant violated its duty of good faith and fair dealing.

127. Plaintiff and Members of the Class have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT

128. Plaintiff and Members of the Classes incorporate the above allegations as if fully set forth herein.

129. This claim is pleaded in the alternative to the breach of express/implied contractual duty claim.

130. Plaintiff and Members of the Classes conferred a benefit upon Defendant in the form of payment in exchange for retirement benefits.

131. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Members of the Class. Defendant also benefited from the receipt of Plaintiff's and Members of the Class's Personal Information, as this was required to facilitate the process of enrolling in a retirement plant.

132. As a result of Defendant's conduct, Plaintiff and Members of the Class suffered actual damages in an amount equal to the difference in value between the payment they provided with reasonable data privacy and security practices and procedures that Plaintiff and Members of the Classes were entitled to, and that payment without unreasonable data privacy and security practices and procedures that they received.

133. Under principals of equity and good conscience, Defendant should not be permitted to retain the monetary value payment belonging to Plaintiff and Members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself for which Plaintiff and Members of the Classes paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

134. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY

135. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

136. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class Members by disclosing and exposing Plaintiff's and the Class Members' Personal Information to enough

people that it is reasonably likely those facts have and/or will become known to the public at large, including, without limitation, on the dark web and elsewhere.

137. The disclosure of current and prospective customers' full names, Social Security numbers, and financial information, is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

138. Defendant has a special relationship with Plaintiff and the Class Members and Defendant's disclosure of Personal Information is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber-criminals who stole the Personal Information would fraudulently misuse that Personal Information, and further sell and disclose the data, just as they are doing. That the original disclosure is devastating to the Plaintiff and the Class Members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large considering that said non-public information is now made public, and cannot be secured again.

139. The tort of invasion of privacy is recognized in Ohio. *See Eysoldt v. ProScan Imaging,* 194 Ohio App.3d 630, 957 N.E.2d 780, 786-87 (1st Dist.). Plaintiff's and the Class Members' Personal Information was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the Class Members' PII is not a matter of legitimate public concern.

140. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages, as set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JOY DRYER, individually and on behalf of all others similarly

situated, the Class as heretofore identified, respectfully prays this Honorable Court for judgment as follows:

A. Certification for this matter to proceed as a class action on behalf of the proposed Class under Fed. R. Civ. Proc. 23;

B. Designation of Plaintiff as Class Representatives and designation of the undersigned as Class Counsel;

C. Actual damages in an amount according to proof;

D. Injunctive or declaratory relief;

E. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

F. Costs and disbursements assessed by Plaintiff in connection with this action, including reasonable attorneys' fees pursuant to applicable law;

G. For attorneys' fees under the common fund doctrine and all other applicable law; and

H. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, hereby demand a trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: October 20, 2022

Respectfully submitted,

/s/ Alyson S. Beridon

Alyson Steele Beridon (#87496)
BRANSTETTER,
STRANCH & JENNINGS,
PLLC
425 Walnut St. Suite 2315
Cincinnati, Ohio 45202
Phone: (513) 381-2224
alysonb@bsjfirm.com

Samuel Strauss*
Raina Borelli*
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
Ph: (608) 237-1775
Email: Sam@turkestrauss.com
Email: AustinD@turkestrauss.com

Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
martys@bsjfirm.com
peterj@bsjfirm.com

*motion for admission pursuant to Fed. R. Civ. Proc. 89(b) to be made

Counsel for Plaintiff and the Proposed Class

ClassAction.org
