IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

BARBARA MENICHINI, individually, and on behalf of all others similarly situated, Plaintiff, v. AMERICAN WATER WORKS COMPANY, INC., Defendant.	Case No. **COMPLAINT — CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Barbara Menichini, individually, and on behalf of all similarly situated persons, alleges the following against Defendant American Water Works Company, Inc. ("American Water" or "Defendant"), based on personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' ("Class Members," as defined *infra*) sensitive personally identifiable information—

i.e., information that is or could be used, whether on its own or in combination with other information, to identify, locate, or contact a person, including, without limitation: names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers ("SSN"), drivers' license information, bank account and other financial information, account information, and other personally identifying information (collectively, "PII").

2. American Water is a New Jersey-based water and wastewater utility company that provides essential water and wastewater services to more than 14 million people across 14 states.[1]

3. In its regulatory filing with the U.S. Securities and Exchange Commission ("SEC"), American Water reported that on October 3, 2024, American Water "learned of unauthorized activity within its computer networks and systems" which it "determined to be the result of a cybersecurity incident" (the "Data Breach"). Upon learning of the Data Breach, American Water "immediately activated its incident response protocols and third-party cybersecurity experts to assist with containment and mitigation activities and to investigate the nature and scope of the incident."[2] American Water also "promptly notified law enforcement

[1] *About American Water*, https://amwater.com/corp/About-Us/ (last visited Oct. 10, 2024).

[2] American Water Works Company, Inc., Current Report (Form 8-K) (Oct. 7, 2024), available at:

and is coordinating fully with them" and "has taken and will continue to take steps to protect its systems and data."

4. American Water also publicly disclosed the Data Breach via an "IT SECURITY FAQS" webpage posted its website on or about October 7, 2024 (the "Website Notice"). On its website, American Water stated that "in an effort to protect our customers' data and to prevent any further harm to our environment, we disconnected or deactivated certain systems" and "proactively took our customer portal service, MyWater, offline, which means we are pausing billing until further notice." American Water added that it was "working diligently to bring these systems back online safely and securely" and "will share information when and as appropriate."[3]

5. Defendant failed to adequately protect Plaintiff's and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The

---

https://www.sec.gov/Archives/edgar/data/1410636/000119312524233300/d869346d8k.htm?7194ef805fa2d04b0f7e8c9521f97343.

[3] *IT Security FAQs – Reactivation of Systems*, American Water, https://amwater.com/corp/security-faq (last visited Oct. 10, 2024).

present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

6. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) adequately vet its data security practices; (ii) warn Plaintiff and Class Members of American Water's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal law.

7. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to ensure that American Water had adequate and reasonable safeguards and measures in place to protect the PII of Plaintiff and Class Members after that information was transferred and entrusted to it in the regular course of business. More specifically, American Water failed to take and implement available steps to prevent an unauthorized disclosure of data, and failed to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption, storage, and destruction of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third parties.

8. Plaintiff and Class Members have a continuing interest in ensuring that

their information is and remains safe in any further transfers of their sensitive data to third parties and they should be entitled to injunctive and other equitable relief.

9. Plaintiff and Class Members have suffered injury as a result of American Water's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

10. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose PII was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

11. Plaintiff Barbara Menichini is a citizen and resident of Pittston, Pennsylvania. Plaintiff is a customer of American Water. Plaintiff provided her PII to American Water as a condition to opening and maintaining an account with

American Water and to receive American Water's services.

12. Defendant American Water Works Company, Inc. is a Delaware corporation with its principal place of business located at 1 Water Steet, Camden, New Jersey 08102.

III. JURISDICTION AND VENUE

13. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class Members who are diverse from Defendant, and (4) there are more than 100 Class Members.

14. The Court has general personal jurisdiction over Defendant because Defendant has its principal place of business in this District.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business*

16. American Water is the largest regulated water and wastewater utility company in the United States.[4] Founded in 1886, American Water provides essential

[4] *About American Water*, American Water, https://amwater.com/corp/About-Us/ (last visited Oct. 10, 2024).

water and wastewater services to more than 14 million people with regulated operations in 14 states and on 18 military installations. As one of the fastest growing utilities in the U.S., American Water expects to invest $34 to $38 billion in infrastructure repairs and replacement, system resiliency and regulated acquisitions over the next 10 years.[5]

17. In the regular course of its business, American Water collects highly private PII from its customers and other individuals who interact or otherwise transact with American Water for business purposes. American Water stores this highly sensitive information digitally.

18. The Customer Privacy Policy available on American Water's website describes the various types of highly sensitive PII it collects as part of its business[6]:

- **Identifiers: contact and account information.** We may collect your name, email address, postal address, and phone number. We may also collect information you provide to create an account or profile.
- **Commercial Information:**
  - **Customer service and feedback.** We may collect information from you when you request customer support or information from us, provide feedback or reviews about your experience with us, or otherwise communicate with or contact us.
  - **Location Information:** In accordance with your device permissions, we may collect or infer information about the location of your device based on your zip code or IP

[5] *Id.*

[6] *Customer Privacy Policy*, American Water, https://amwater.com/corp/resources/PDF/Data-Privacy/American-Water-Privacy-Policy.pdf (last visited Oct. 10, 2024).

address.

- **Internet or other electronic network activity information:** We collect information about how you access our Service, including technical data about the device and network you use, such as your hardware model, operating system version, mobile network, IP address, unique device identifiers, browser type, and app version. We also collect information about your activity on our Service, such as login attempts, logout events, access times, pages and data viewed, links clicked, and the page you visited before navigating to our Service.
- **Data underlying any errors that may occur during your use of the Service.**

Sensitive Information: Special categories of particularly sensitive personal data require higher levels of protection depending on local law. In some rare cases, we may collect sensitive personal data about individuals. Please note that, where permitted by law, we may collect, store, and use sensitive information about you, including race, ethnicity, veteran status, disability status, gender, sex, age, marital status, and health and medical conditions. Please be assured that we will only use such sensitive information for the purposes set out in this Policy, or as otherwise described to you at the time such information is collected, and in accordance with applicable law.

19. Upon information and belief, the PII held by American Water in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

20. American Water makes a host of claims about data security on its website—*www.amwater.com*—including promises and representations to its customers and other related individuals, that the PII collected from them, including that of Plaintiff and Class Members, would be kept safe and confidential, that the privacy of that information would be maintained in accordance with industry

standards and the law, and that it would delete any sensitive information after it was no longer required to maintain it.

21. For example, the Customer Privacy Policy ensures consumers that American Water is "committed to protecting the privacy and security of [their] data."[7] It states:

> We make reasonable efforts to ensure a level of security appropriate to the risk associated with the processing of personal data. We maintain organizational, technical, and administrative measures designed to protect personal data within our organization against unauthorized access, destruction, loss, alteration or misuse.[8]

22. American Water also claims to be "the first U.S. water and wastewater company and the third utility to earn the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act designation."[9] American Water's website further states:

> American Water recognizes the essentiality of our water and wastewater services and acknowledges the severity of cyber threats. Our company has always endorsed a "safety and security approach" to water and wastewater operations, and this persistence extends to cyber threats as well. We have taken several steps to help maintain the security of our systems and work with local, state, and federal government agencies to prepare for cyber threats.
>
> Additionally, American Water has a dedicated team of certified professionals who help maintain the cybersecurity of our informational

[7] *Customer Privacy Policy*, n.6, *supra*.
[8] *Id.*
[9] *Support Anti-Terrorism by Fostering Effective Technologies (Safety)*, American Water, https://amwater.com/corp/About-Us/Safety/cybersecurity (last visited Oct. 10, 2024).

> and operational technology systems, safeguard the physical security of our staff, facilities and assets, and provide emergency response and business continuity activities. We recognize cyber threats' sophistication and focus on understanding and minimizing impact if a breach occurs by constantly testing our cyber response protocols.[10]

23. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

24. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant had a legal duty to keep its customers' PII safe and confidential.

25. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

26. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members'

[10] *Id.*

PII from disclosure.

B. *The Data Breach*

28. According to its regulatory filing with the SEC, on October 3, 2024, American Water "learned of unauthorized activity within its computer networks and systems" which was determined to be the result of a cybersecurity incident.[11] Upon learning of the Data Breach, American Water "immediately activated its incident response protocols and third-party cybersecurity experts to assist with containment and mitigation activities and to investigate the nature and scope of the incident."[12] American Water also "promptly notified law enforcement and is coordinating fully with them" and "has taken and will continue to take steps to protect its systems and data."[13]

29. American Water also publicly disclosed the Data Breach via an "IT SECURITY FAQS" webpage posted its website on or about October 7, 2024. On the Website Notice, American Water stated that "in an effort to protect our customers' data and to prevent any further harm to our environment, we disconnected or deactivated certain systems" and "proactively took our customer portal service, MyWater, offline, which means we are pausing billing until further notice." American Water added that it was "working diligently to bring these

[11] *See* Form 8-K, n.2, *supra*; Website Notice.
[12] *Id.*
[13] *Id.*

systems back online safely and securely" and "will share information when and as appropriate."[14]

30. On October 10, 2024, American Water provided an update via an "IT SECURITY FAQS – REACTIVATION OF SYSTEMS" webpage posted on its website, which stated:

> American Water is in the process of methodically and securely reconnecting and reactivating systems following a recent cybersecurity incident. **At this time, our customer portal, MyWater, is now securely back online and customers can resume using this platform as normal**. We sincerely regret any inconvenience this has caused and appreciate your patience as we worked to restore these services.
>
> As always, providing safe and reliable access to water and wastewater services is our top priority – and we continue to have no indication that any of our water or wastewater facilities or operations have been negatively impacted by this incident.[15]

31. Omitted from both the Form 8-K Filing and Website Notice are the details of the root cause of the Data Breach, the vulnerabilities exploited, and the specific remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

32. These "disclosures" amount to no real disclosure at all, as they fail to inform, with any degree of specificity, Plaintiff and Class Members of the Data

[14] *IT Security FAQs – Reactivation of Systems*, n.3, *supra.*
[15] *Id.*

Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

33. 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 PII. Nor did Defendant take the precautions and measures needed to ensure American Water's data security protocols were sufficient to protect the PII in its possession.

34. The attacker accessed and acquired files containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

35. Plaintiff further believes her PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

C. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII*

36. American Water derives a substantial economic benefit from providing services to its customers, and as a part of providing those services, Defendant retains and stores the PII of its customers and of other individuals who interact or otherwise transact with American Water for business purposes, including that of Plaintiff and Class Members.

37. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from disclosure, and making sure the PII was safe in the hands of any vendors to which American Water provided that highly sensitive information.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

39. Plaintiff and Class Members relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, to provide the information to trusted and secure vendors and other third parties, and to make only authorized disclosures of this information.

40. Defendant could have prevented this Data Breach by properly securing the PII of Plaintiff and Class Members and ensuring that its vendors did the same.

41. Upon information and belief, Defendant made promises to consumers to maintain and protect PII, demonstrating an understanding of the importance of securing PII.

42. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. *Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of PII Are Particularly Susceptible to Cyberattacks*

43. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

44. Data thieves regularly target companies that receive and maintain PII due to the highly sensitive nature of that information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

45. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[16]

46. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known the PII it collected and maintained would be targeted by

[16] *See* 2021 Data Breach Annual Report, at 6, IDENTITY THEFT RESOURCE CENTER (Jan. 2022), https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf.

cybercriminals.

47. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

48. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it collected and maintained and, thus, the significant number of individuals who would be harmed by the exposure of that data.

49. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

50. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members, and Defendant's failure to adequately vet its vendors.

51. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long-lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

E. *Value of Personally Identifiable Information*

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[17] The FTC describes "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."[18]

53. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[19]

54. For example, PII can be sold at a price ranging from $40 to $200.[20] Criminals can also purchase access to entire company data breaches from $900 to

---

[17] 17 C.F.R. § 248.201 (2016).
[18] *Id.*
[19] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[20] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

$4,500.[21]

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

56. This data demands a much higher price on the black market. 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."[22]

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

58. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when

[21] *In the Dark*, VPNOVERVIEW.COM, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 8, 2024).
[22] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, NETWORK WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

F. *Defendant Failed to Comply with FTC Guidelines*

59. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

60. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to

[23] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Report to Congressional Requesters*, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

61. The FTC further recommends that companies not maintain PII 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, and those of its vendors. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice

prohibited by Section 5 of the FTCA.

64. Defendant was at all times fully aware of its obligation to protect the PII it was entrusted with, yet failed to comply with such obligation. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. *Defendant Failed to Comply with Industry Standards*

65. As noted above, experts studying cybersecurity routinely identify institutions like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which it collects and maintains.

66. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like American Water, include, but are not limited to: educating all employees; strong password requirements; multilayer security, including firewalls; anti-virus and anti-malware software; encryption; multi-factor authentication; backing up data; and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all these industry best practices.

67. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding

these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

68. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

69. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

H. *Defendant Breached Its Duties to Safeguard Plaintiff's and Class Members' PII*

70. In addition to its obligations under federal laws, Defendant owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members.

71. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner.

72. Defendant owed a duty to Plaintiff and Class Members to properly vet all third parties to whom it provided its customers' and other related individual's highly sensitive PII.

73. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

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

75. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately vet its vendors to ensure they maintained sufficient data security practices;

b. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

c. Failing to adequately protect customers' and other related individuals' PII;

d. Failing to properly monitor its own data security systems for existing intrusions;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

76. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

77. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

I. *Common Injuries & Damages*

78. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has

materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of the value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of American Water, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

J. *The Data Breach Increases Victims' Risk of Identity Theft*

79. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

80. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

81. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft-

related crimes discussed below.

82. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

83. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's log-in credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

84. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[24]

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which

85. With "Fullz" packages, cybercriminals 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 to assemble complete dossiers on individuals.

86. The development of "Fullz" packages means that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, driver's license numbers, 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 that was exfiltrated in the Data Breach, criminals may still 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.

K. *Loss of Time to Mitigate Risk of Identity Theft and Fraud*

87. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised,

---

are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, KREBSONSECURITY.COM BLOG (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

88. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

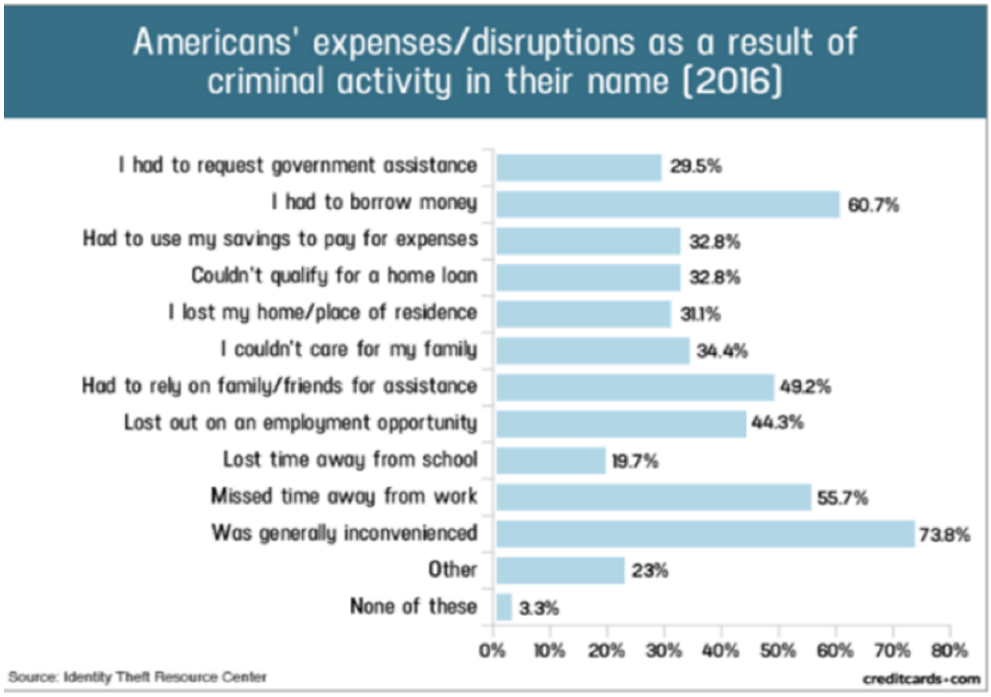
89. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

90. These efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after

[25] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf

a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[26]

91. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



L. *Diminution of Value of PII*

92. PII is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyberthefts include

[26] *See* Federal Trade Commission, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Steps (last visited Oct. 8, 2024).

heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that PII has considerable market value.

93. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[27]

94. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[28]

95. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[29]

96. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[30]

97. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this

---

[27] David Lazarus, *Shadowy data brokers make the most of their cloak,* LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[28] DATACOUP, https://datacoup.com/ (last visited Oct. 8, 2024).

[29] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at: https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visit Oct. 8, 2024).

[30] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

M. *Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary*

98. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchased by criminals intending to utilize the PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

99. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

100. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

101. The retail cost of credit monitoring and identity theft monitoring can

cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost, for a minimum of five years, that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

N. ***Plaintiff's Experience***

102. Plaintiff is a customer of American Water. Plaintiff provided her PII to American Water as a condition to opening and maintaining an account with American Water and to receive American Water's services.

103. Plaintiff provided her PII to American Water and trusted the company would use reasonable measures to protect it according to its policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

104. At the time of the Data Breach, Defendant collected and retained Plaintiff's and Class Members' PII in its systems.

105. Plaintiff's and Class Members' PII was compromised in the Data Breach and stolen by cybercriminals.

106. Plaintiff has been injured by the compromise of her PII.

107. Plaintiff takes reasonable measures to protect her PII. She has never

knowingly transmitted unencrypted PII over the internet or other unsecured source.

108. Plaintiff stores any documents containing her PII in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

109. Had Plaintiff known that American Water does not adequately protect PII, she would not have agreed to provide her sensitive PII to Defendant and would not have agreed to be a customer of American Water.

110. Plaintiff recently has incurred unauthorized charges on her debit card. In or around August 2024, Plaintiff incurred an unauthorized charge of $146 from Sirius XM on her debit card. Plaintiff contacted Sirius XM about obtaining a refund for the unauthorized charge but was unsuccessful. Plaintiff then reported the unauthorized charge to her credit union as fraud. Plaintiff's credit union thereafter canceled her debit card and issued a replacement card.

111. As a result of and following the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach to protect herself from identity theft and fraud. She has monitored, and continues to monitor, her accounts, credit reports and credit scores, and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

112. And in the aftermath of the Data Breach, Plaintiff has suffered from a

spike in spam and scam text messages and phone calls. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach. Because of the Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

113. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that was entrusted to Defendant, which was compromised in and as a result of the Data Breach.

114. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

115. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals that will continue for her lifetime.

116. Defendant obtained and continues to maintain Plaintiff's PII, and thus has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

117. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address

harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

118. Further, Plaintiff is and will remain at risk of harm in the future because American Water continues to maintain her confidential PII but does not take adequate steps to protect that information from a data breach. Accordingly, Plaintiff's PII faces an imminent risk of disclosure in a future American Water data breach.

V. CLASS ALLEGATIONS

119. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks certification of the following classes (together, the "Class"):

> **Nationwide Class**
> All individuals residing in the United States whose PII was compromised in the Data Breach, including all individuals who received notice of the Data Breach.
>
> **Pennsylvania Class**
> All individuals residing in Pennsylvania whose PII was compromised in the Data Breach, including all individuals who received notice of the Data Breach.

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

and immediate family members.

121. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

122. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

123. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes millions of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

124. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendant owed duties to Class Members to safeguard their PII;

h. Whether Defendant breached its duties to Class Members to safeguard their PII;

i. Whether hackers obtained Class Members' PII via the Data Breach;

j. Whether Defendant had legal duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached implied contracts with Plaintiff and

Class Members;

p. Whether Defendant was unjustly enriched;

q. Whether Plaintiff and Class Members are entitled to damages;

r. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

125. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Defendant's common misconduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

127. Predominance. Defendant has engaged in common courses of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

128. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

129. Class certification is also appropriate under Federal Rule of Civil

Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

130. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names, email and/or postal addresses, and phone numbers of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I
Negligence and Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class, or in the Alternative, the Pennsylvania Class, Against American Water)

131. Plaintiff incorporates and realleges paragraphs 1-130 as if fully set forth herein.

132. Plaintiff and Class Members provided their PII to Defendant as a condition of receiving services.

133. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

134. By assuming the responsibility to collect and store this data, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

135. Defendant had a duty to employ reasonable security measures under

Section 5 of the FTCA, 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.

136. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

137. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

138. Defendant had and continues to have duties to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

139. Defendant breached its duties, pursuant to the FTCA and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. 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' PII, including in choosing its vendors;

b. Failing to hold vendors with whom it shared sensitive PII to adequate standards of data protection;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

140. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect 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 it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

141. Plaintiff and Class Members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm this statute was intended to guard against.

142. Defendant's violation of Section 5 of the FTCA constitutes negligence per se.

143. The FTC has pursued enforcement actions against businesses, which, 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 Class Members.

144. Defendant breached its duties to Plaintiffs and Class Members under Section 5 of the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

145. Plaintiffs and Class Members were foreseeable victims of Defendant's violations of Section 5 of the FTCA.

146. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

147. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches at large corporations that collect and store PII.

148. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were

wrongfully disclosed.

149. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on its systems.

150. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

151. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

152. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

153. Defendant's duties extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

154. Defendant has admitted that the PII of Plaintiff and Class Members was

wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

155. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

156. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

157. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate

and adequate measures to protect the PII.

158. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

159. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

160. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

161. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

162. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or in the Alternative, the Pennsylvania Class, Against American Water)

163. Plaintiff incorporates and realleges paragraphs 1-130 as if fully set forth herein.

164. Defendant offered to provide services to its customers, including Plaintiff and Class Members, in exchange for payment.

165. Defendant also required Plaintiff and Class Members to provide it with their PII in order to receive services.

166. In turn, Defendant impliedly promised to protect Plaintiff's and Class Members' PII through adequate data security measures.

167. Plaintiff and Class Members accepted Defendant's offer by providing their valuable PII to Defendant in exchange for Plaintiff and Class Members receiving Defendant's services, and then by paying for and receiving the same.

168. Plaintiff and Class Members would not have done the foregoing but for the above-described agreement with the company.

169. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant in exchange for, amongst other things, the protection of such information.

170. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

171. However, Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

172. In sum, Plaintiff and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

173. As a reasonably foreseeable result of the Data Breach, Plaintiff and Class Members were harmed by Defendant's failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

174. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class, or in the Alternative, the Pennsylvania Class, Against American Water)

175. Plaintiff incorporates and realleges paragraphs 1-130 as if fully set forth herein.

176. This count is brought in the alternative to Plaintiff's breach of express and/or implied contract claims.

177. Upon information and belief, Defendant funds its data security

measures entirely from its general revenue, including from payments made by or on behalf of its customers for services.

178. As such, a portion of the value and monies derived from payments made by its customers for services is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

179. Plaintiff and Class Members conferred a monetary benefit on Defendant in providing it with their valuable PII.

180. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

181. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profit over the requisite security.

182. Defendant failed to secure Plaintiff's and Class Members' PII and,

therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

183. Under the principles of equity and good conscience, Defendant should not be permitted to retain the benefits that Plaintiff and Class Members conferred upon it.

184. Plaintiff and Class Members have no adequate remedy at law.

185. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

186. 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 Plaintiff and Class Members may seek restitution or compensation.

COUNT IV
Declaratory and Injunctive Relief, 28 U.S.C. § 2201
(On Behalf of Plaintiff and the Nationwide Class, or in the Alternative, the Pennsylvania Class, Against American Water)

187. Plaintiff incorporates and realleges paragraphs 1-130 as if fully set forth herein.

188. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

189. Defendant owes a duty of care to Plaintiff and Class Members that required it to adequately secure their PII.

190. Defendant still possesses Plaintiff's and Class Members' PII, yet does not adequately protect PII against the threat of a data breach.

191. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members.

192. Actual harm has arisen in the wake of the Data Breach regarding Defendant's obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's ongoing failure to address the security failings that led to such exposure.

193. There is no reason to believe that Defendant's employee training and

security measures are any more adequate now than they were before the breach to meet its obligations and legal duties.

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

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

c. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

d. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

e. ordering that Defendant audit, test, and train its security personnel and

employees regarding any new or modified data security policies and procedures;

f. ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Personal Information not necessary for its provision of services;

g. ordering that Defendant conduct regular database scanning and security checks; and

h. prohibiting Defendant from maintaining PII of Plaintiff and Class Members on a cloud-based database;

i. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

j. ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive PII;

k. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding paragraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies,

programs, and systems for protecting personal identifying information;

l. requiring Defendant to meaningfully educate all class members about the threats they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

m. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

n. such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court enter an Order:

A. Certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. Granting equitable relief and enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. Granting injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: October 14, 2024

Respectfully submitted,

By: */s/ Andrew Ferich*

Andrew W. Ferich (NJ I.D. 015052012)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Bradley K. King (NJ I.D. 081472013)
AHDOOT & WOLFSON, PC
521 5th Avenue, 17th Floor
New York, NY 10175
Telephone: (917) 336-0171
Facsimile: (917) 336-0177
bking@ahdootwolfson.com

Counsel for Plaintiff and the Putative Class

CERTIFICATION PURSUANT TO LOCAL CIVIL RULE 11.2

Pursuant to L. Civ. R. 1 1.2, I hereby certify to the best of my knowledge that the matter in controversy is not the subject of any other action pending in any court or the subject of a pending arbitration proceeding, nor is any other action or arbitration proceeding contemplated. I further certify that I know of no party, other than putative class members, who should be joined in the action at this time.

Dated: October 14, 2024

/s/ Andrew W. Ferich
Andrew W. Ferich

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: American Water Data Breach Lawsuit Filed in New Jersey Over 2024 Cyberattack

---