IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JUN HEE KIM, ON BEHALF OF HIMSELF AND ALL OTHERS SIMILARLY SITUATED, Plaintiff, v. WP COMPANY LLC D/B/A THE WASHINGTON POST, Defendant.	Case No.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jun Hee Kim ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against WP Company LLC d/b/a The Washington Post ("Defendant"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

NATURE OF THE ACTION

1. This class action arises out of Defendant's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiff's and Class members' sensitive personally identifiable information that it had acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack to take place between July 10, 2025, and August 22, 2025, to compromise Defendant's network (the "Data Breach") that contained Private Information, including Personally Identifiable Information ("PII"). According to the notice Plaintiff received in the mail ("the Notice"), the types of personal data

exposed included names, employee ID numbers, bank account numbers, and routing numbers.[1] Approximately 10,000 employees and contractors had their personal and financial data exposed as a consequence of the Breach.[2]

3. Defendants learned of the Data Breach on or around October 27, 2025, and determined that Class members' Private Information had been compromised. Yet, Defendants unreasonably delayed notifying affected issues, failing to begin issuing its Notice of Data Breach letters until November 12, 2025.[3]

4. On its computer network, Defendant holds and stores certain highly sensitive PII of Plaintiff and the putative Class members, individuals who provided their highly sensitive and private information in exchange for employment.

5. As a result of Defendant's Data Breach, Plaintiff and thousands of Class members suffered ascertainable losses in the form of financial losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. In addition, Plaintiff's and Class members' highly sensitive Personal Information, which was entrusted to Defendant, was compromised, unlawfully accessed, and exfiltrated as a result of the Data Breach.

7. Based upon the Notice, the Data Breach was caused by a cybercriminal gaining access to Defendant's Oracle E-Business Suite applications.[4] The Notice provided that "Oracle had identified a previously unknown and widespread vulnerability in its E-Business Suite software

[1] *See* Plaintiff's Notice Letter, Exhibit 1.
[2] *See* Bill Toulas, *Washington Post data breach impacts nearly 10k employees, contractors*, BLEEPING COMPUTER (Nov. 13, 2025), https://www.bleepingcomputer.com/news/security/washington-post-data-breach-impacts-nearly-10k-employees-contractors/.
[3] Plaintiff's Notice Letter, Exhibit 1.
[4] *Id.*

that permitted unauthorized actors to access many Oracle customers' E-Business Suite applications."[5]

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff and Class members' Private Information, as well as Defendant's failure to utilize software used for HR and other business purposes which has adequate and reasonable cybersecurity procedures.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

10. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network and in its Oracle application environment in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

11. Defendant disregarded the privacy and property rights of Plaintiff and Class members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust systems and security practices to safeguard

[5] *Id.*

Class members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class members prompt, accurate, and complete notice of the Data Breach.

12. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner and potentially been able to mitigate the injuries to Plaintiff and the Class.

13. Plaintiff's and Class members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' information, filing false medical claims using Class members' information, obtaining driver's licenses in Class members' names with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class members may also incur out-of-pocket expenses for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself, and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

18. Accordingly, Plaintiff brings this action against Defendant for negligence, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for Defendant's unlawful conduct.

19. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket expenses, and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate, long-term credit monitoring services funded by Defendants, and declaratory relief.

PARTIES

Plaintiff Jun Hee Kim

20. Plaintiff Jun Hee Kim is and at all times relevant to this Complaint an individual citizen in the state of Maryland, residing in the city of Boyds. Plaintiff Kim was an employee of Defendant from 2018 through 2019.

Defendant Washington Post

21. Defendant The Washington Post is a daily newspaper located at 1301 K Street NW, Washington, D.C., 20071. Defendant can be served through its registered agent CT Corporation System located at 1015 15th Street NW, Suite 1000, Washington, D.C., 20005.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value

of $5,000,000, exclusive of interest and costs, there are more than 100 members in the putative Class, and at least one member of the Class is a citizen of a state different from Defendant.

23. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendants operate, conduct, engage in, or carry on a business in the District of Columbia; they are registered with the District of Columbia Department of Licensing and Consumer Protection as a corporation; they maintain their headquarters in the District of Columbia; and committed tortious acts in the District of Columbia.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Defendant has the most significant contacts and because a substantial portion of the acts and omissions that give rise to the claims herein occurred in this district.

FACTS

25. Defendant is a daily newspaper originally founded in 1877, now offering both print and digital publications.[6] As an employer, Defendant was entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable law and industry standards.

26. Employees provide their Private Information to Defendant with the mutual understanding that this highly sensitive information was confidential and would be properly safeguarded from misuse and theft.

27. In the course of collecting Private Information from former and current employees, including Plaintiff and Class members, Defendant promised to provide confidentiality and adequate security for Private Information through their legal obligations to be in compliance with

[6] *Washington Post company history*, THE WASHINGTON POST, https://www.washingtonpost.com/company-history/ (last visited Nov. 19, 2025).

statutory privacy requirements. Defendants are aware of and have obligations created by the Federal Trade Commission Act ("FTCA"), contract, industry standards, and common law to keep Plaintiff's and Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

28. Consumers and employees, in general, demand that businesses that require highly sensitive Private Information provide adequate security to safeguard that information.

29. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class members' PII from unauthorized disclosure to third parties.

The Data Breach

30. On or around November 12, 2025, Plaintiff received a Notice from Defendant stating that on October 27, 2025, it learned that "some of [Plaintiff's] personal information was potentially affected by a data security incident involving a previously unknown vulnerability affecting certain software from Oracle."[7] The Notice stated that the Breach occurred between July 10, 2025, and August 22, 2025.[8] The Notice provided that "Oracle had identified a previously unknown and widespread vulnerability in its E-Business Suite software that permitted unauthorized actors to access many Oracle customers' E-Business Suite applications."[9]

31. Plaintiff's and Class members' Private Information was in the hands of cybercriminals for approximately three months before Defendant learned of the Breach, and then another more than two weeks before Defendant notified Plaintiff and Class members.

[7] Plaintiff's Notice Letter, Exhibit 1.
[8] *Id.*
[9] *Id.*

32. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiff and Class members.

33. Upon information and belief, the Private Information stored on Defendant's network was not encrypted.

34. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff reasonably believes his stolen Private Information is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

35. Plaintiff's Notice stated that his name, employee ID number, bank account number, and routing number may have been compromised in the Data Breach.[10] Defendant recommends several steps that Plaintiff and Class members can take to protect their Personal Information, including: reviewing account statements and notifying law enforcement of suspicious activity, monitoring their credit reports at least monthly, placing a fraud alert on their credit report, and putting a security freeze on their credit file.[11] Plaintiff's Notice does not contain any information regarding credit monitoring or other services Defendant will pay for to protect Plaintiff's and Class members' Personal Information.

36. That Defendant is encouraging Plaintiff and Class members to review their credit reports, bank accounts, and suggesting they place a fraud alert on their credit report, is an acknowledgment that the impacted former and current employees are subject to a substantial and imminent threat of fraud and identity theft.

[10] *Id.*
[11] *Id.*

37. Defendant had obligations created by contract, industry standards, and common law to keep Plaintiff's and Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

38. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Personal Information, as well as selecting third-party software for business purposes which has adequate and reasonable cybersecurity procedures

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information

39. Defendant acquires, collects, and stores a massive amount of Private Information from whom they are providing employment.

40. By obtaining, collecting, and using Plaintiff's and Class members' PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

41. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information.

42. Plaintiff and Class members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach was a Foreseeable Risk for which Defendant Was on Notice

43. It is well known that PII is a valuable commodity and a frequent, intentional target of cybercriminals. Companies that collect such information, including Defendant, are well aware of the risk of being targeted by cybercriminals.

44. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, including severe distress and hours of lost time trying to fight against the impact of identity theft.

45. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[12]

46. In 2024, there were 3,158 data breaches recorded, similar to the 3,205 breaches reported in 2023. However, the number of victims affected jumped to 1.35 billion people, a 211% increase from 2023 to 2024.[13]

47. A report issued by Ivanti interviewed "more than 2,400 security leaders and found that the top predicted threat for 2025 is ransomware. According to the report, nearly 1 out of every 3 security professionals (38%) believe ransomware will become an even greater threat when powered by AI."[14] This is particularly alarming as nation-states and cybercriminals grow more

[12] Erika Harrell, *Victims of Identity Theft*, 2018, U.S. DEPARTMENT OF JUSTICE BULLETIN at 9 (Apr. 2021), https://bjs.ojp.gov/document/vit18.pdf.
[13] *Identity Theft Resource Center's 2024 Annual Data Breach Report Reveals Near-Record Number of Compromises and Victim Notices*, IDENTITY THEFT RESOURCE CENTER (Jan. 28, 2025), https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/.
[14] Chuck Brooks, *Key Cybersecurity Challenges in 2025—Trends and Observations*, FORBES (Apr. 5, 2025), https://www.forbes.com/sites/chuckbrooks/2025/04/05/key-cybersecurity-challenges-in-2025-trends-and-observations/.

sophisticated. Unfortunately, these preventable causes will largely come from businesses with a "lack of cybersecurity expertise and significant security resources."[15]

48. In light of 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 that its computer network would be targeted by cybercriminals.

49. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, prepared for, and hopefully can ward off a cyberattack. According to an FBI publication, "[r]ansomware is a type of malicious software—or malware—that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[16] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[17]

50. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgments of data security compromises, and its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

---

[15] *Id.*
[16] *Ransomware*, FEDERAL BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware (last visited Oct. 6, 2025).
[17] *Id.*

At All Relevant Times, Defendant Had a Duty to Plaintiff and Class Members to Properly Secure Their Private Information

51. At all relevant times, Defendant had a duty to Plaintiff and Class members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class members, and to promptly notify Plaintiff and Class members when Defendant became aware that their PII was compromised.

52. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class members.

53. Security standards commonly accepted among businesses that store PII using the Internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PHI;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor Exit Nodes.

54. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] 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."[19]

55. The ramifications of Defendant's failure to keep former and current employees' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims including Plaintiff and the Class may continue for years.

The Value of Personally Identifiable Information

56. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[20]

57. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[21]

58. This data, as one would expect, demands a much higher price on the black market. Martin Walter, Senior Director at cybersecurity firm RedSeal, explained, "[c]ompared to credit

[18] 17 C.F.R. § 248.201(b)(9).
[19] 17 C.F.R. § 248.201(b)(8).
[20] 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/.
[21] *In the Dark*, VPN OVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 6, 2025).

card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[22]

59. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[23]

60. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class members' PII can easily obtain Class members' tax returns or open fraudulent credit card accounts in Class members' names.

61. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change.

62. Defendant's credit monitoring advice included in the Notice squarely places the burden on Plaintiff and Class members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiff and Class members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class members in credit monitoring services upon discovery of the Data Breach, Defendant merely sent instructions to Plaintiff and Class members about actions they can take to retroactively protect themselves.

---

[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/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[23] *Memorandum from Clay Johnson III, Deputy Director for Management, Office of Management and Budget, on Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, n.1 (May 22, 2007), *available at* https://whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2007/m07-16.pdf.

63. These suggestions are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. They also entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class members' PII.

64. 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 victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

65. Federal and state governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

66. 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.[25] The guidelines note businesses should protect the personal consumer and employee information that they keep, as well as 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 security problems.

[24] *Start with Security*, FEDERAL TRADE COMMISSION (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[25] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business-0 (last visited Oct. 6, 2025).

67. The FTC emphasizes that early notification to data breach victims reduces injuries, stating that "[i]f you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[26]

68. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[27]

69. The FTC recommends that businesses[28]:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an Internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

[26] *Data Breach Response: A Guide for Business*, FEDERAL TRADE COMMISSION (Aug. 2023), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last visited Oct. 6, 2025).
[27] *See Start with Security, supra* note 24, at 11.
[28] *See Protecting Personal Information, supra* note 25.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the Internet.

g. Determine whether a border firewall should be installed where the business' network connects to the Internet. A border firewall separates the network from the Internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

70. The FTC has brought enforcement actions against businesses for failing to protect employee and consumer data adequately and reasonably, 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 FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. Because Class members entrusted Defendant with their PII, Defendant had, and continues to have, a duty to Plaintiff and the Class to keep their PII secure.

72. Plaintiff and Class members reasonably expected that when they provided PII to Defendant (or to Defendant's customers), Defendant would safeguard their PII.

73. Defendant was at all times fully aware of its obligation to protect the personal and financial data of former and current employees, including Plaintiff and members of the Class. Defendant was also aware of the significant repercussions if they failed to do so.

74. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data—including Plaintiff's and Class members' names, employee ID numbers, bank account numbers, and routing numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Concrete Injuries Were Caused by Defendant's Inadequate Security

75. Plaintiff and Class members reasonably expected that Defendant would provide adequate security protections for their PII, and Class members provided Defendant with sensitive personal information, including their names, bank account numbers, and routing numbers.

76. Defendant's poor data security deprived Plaintiff and Class members of the benefit of their bargain. Plaintiff and other individuals whose PII was entrusted with Defendant understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class

members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff and the Class members suffered pecuniary injury.

77. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff and Class members have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

78. The cybercriminals who obtained the Class members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, employee ID numbers, bank account numbers, routing numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class member's name, including but not limited to:

a. Obtaining employment;

b. Obtaining a loan;

c. Applying for credit cards or spending money;

d. Filing false tax returns;

e. Stealing Social Security and other government benefits; and

f. Applying for a driver's license, birth certificate, or other public document.

79. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class members have been deprived of the value of their PII, for which there is a well-established national and international market.

80. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

81. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class members' PII will do so at a later date or re-sell it.

82. As a result of the Data Breach, Plaintiff and Class members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

Data Breaches Put Victims at an Increased Risk of Fraud and Identity Theft

83. Data breaches, such as the one experienced by Plaintiff and the Class, are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

84. In 2019, the U.S. Government Accountability Office released a report addressing the steps consumers can take after a data breach.[29] Its appendix of steps consumers should consider, in simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options.[30] It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiff and the

[29] *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, Report No. GAO-19-230 (Mar. 2019) at 37-41, *available at* https://www.gao.gov/assets/gao-19-230.pdf (last visited Oct. 6, 2025).
[30] *Id.*

Class) must take after a breach like Defendant's are both time-consuming and of only limited and short-term effectiveness.

85. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 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.[31]

86. It must also be noted that there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies 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.[32]

87. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

88. There is a strong probability that the entirety of the stolen information has been dumped on the dark web or will be dumped on the dark web, meaning Plaintiff and Class members

---

[31] *Identity Theft*, FEDERAL TRADE COMMISSION, https://consumer.ftc.gov/identity-theft-and-online-security/identity-theft (last visited Oct. 6, 2025).

[32] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, Report No. GAO-07-737 (June 2007) at 29, *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 6, 2025).

are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for many years to come.

Plaintiff Kim's Experience

89. Plaintiff Jun Hee Kim is, and has been at all times relevant to this Complaint, a resident and citizen of the state of Maryland.

90. Plaintiff Kim was an employee of the Washington Post from 2018 through 2019. To obtain employment from the Washington Post, Defendant required that Plaintiff Kim provide it with his PII. Defendant was therefore provided with his Personal Information.

91. On or around November 12, 2025, Plaintiff Kim received the Notice, which indicated that Defendant had known about the Data Breach for over two weeks before sending the Notice—and that the Breach had occurred approximately three months before Defendant even became aware. The Notice informed him that his critical Private Information was accessed by an unauthorized actor. The Notice stated that the extracted information included his name, employee ID number, bank account number, and routing number.[33] Plaintiff Kim is alarmed by the amount of his Personal Information that was stolen or accessed.

92. In response to Defendant's Notice, Plaintiff has been and will continue to be required to spend time dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the Notice, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

[33] Plaintiff's Notice Letter, Exhibit 1.

93. Since the Data Breach, Plaintiff Kim has noticed an increase in spam calls and text messages. He receives at least one spam call or text message every day.

94. Immediately after receiving the Notice, Plaintiff Kim spent time evaluating his next steps including consulting with legal counsel, changing his passwords, and checking his financial accounts for a minimum of an hour per week in an effort to mitigate the damage that has been caused by Defendant.

95. Plaintiff Kim is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the Internet or any other unsecured source.

96. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided Defendant with his Private Information had Defendant disclosed that it lacked data security practices adequate to safeguard it.

97. Plaintiff Kim suffered actual injury in the form of damages and diminution in the value of his Private Information – a form of intangible property that he entrusted to Defendant.

98. Plaintiff suffered lost time, annoyance, interference, anxiety, and inconvenience as a result of the Data Breach, as well as increased concerns for the loss of his privacy.

99. Plaintiff Kim reasonably believes that his Private Information may have already been sold to cybercriminals. Had he been notified of Defendant's Data Breach in a timely manner, he could have attempted to mitigate his injuries.

100. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

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

CLASS ACTION ALLEGATIONS

102. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

103. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals whose Private Information was compromised through the Washington Post Data Breach between July 10, 2025, and August 22, 2025.

104. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

105. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

106. **Numerosity**. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately thousands of people whose data was compromised in Data Breach.

107. **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 unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' Private Information;

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

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

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

e. Whether Defendant owed a duty to Class members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class members to safeguard their Private Information;

g. Whether computer hackers obtained Class members' Private Information in the Data Breach;

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

i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's failed to provide notice of the Data Breach in a timely manner; and

l. Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

109. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

110. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that all the Plaintiff's and Class members' Private Information was stored on the same computer systems and unlawfully accessed 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.

111. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. 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 the cost of litigating their individual claims 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, the conduct of 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.

112. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class wide basis.

113. Likewise, particular issues under Fed. R. Civ. P. 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 particular issues include, but are not limited to:

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

b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer and employee Private Information;

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

114. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent Notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

115. Plaintiff incorporates by reference the allegations above as if fully set forth herein.

116. Plaintiff incorporates by reference the allegations above as if fully set forth herein.

117. Defendant gathered and stored the Private Information of Plaintiff and Class members as part of the regular course of its business operations. Plaintiff and Class members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

118. By collecting and storing this data in its computer property, sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

119. 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 Private Information.

120. 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.

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

122. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. 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 the Class.

123. Defendant gathered and stored the Private Information of Plaintiff and Class members as part of its business of soliciting its services to its consumers and hiring employees, which solicitations and services affect commerce.

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

125. Defendant breached its duties to Plaintiff and Class members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' Private Information, and by failing to provide prompt notice without reasonable delay.

126. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations including but not limited to the common law. Defendant alone was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a Data Breach.

127. Defendant's multiple failures to comply with applicable laws and regulations constitute negligence per se.

128. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

129. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class members could and would suffer from if the Private Information was wrongfully disclosed, and the importance of adequate security.

130. Plaintiff and Class members were the foreseeable victims of inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their Private Information that was in Defendant's possession.

131. Defendant was in a special relationship with Plaintiff and Class members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiff and Class members by ensuring that their Private Information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiff's and Class members' Private Information. The harm to Plaintiff and Class members from its exposure was highly foreseeable to Defendant.

132. Defendant owed Plaintiff and Class members a common law duty to use reasonable care to avoid causing a foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

133. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the 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.

134. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to compromise by taking common sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and Class members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

135. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to it.

136. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and Class members' Private Information;

f. Failing to mitigate the harm caused to Plaintiff and the Class members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their Private Information.

137. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

138. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class members have suffered damages and are at imminent risk of additional harms and damages, as alleged above.

139. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class members from being

stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class members while it was within Defendant's possession and control.

140. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their Private Information and mitigate damages.

141. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

142. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

143. The damages Plaintiff and the Class have suffered and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

144. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

145. Plaintiff incorporates by reference the allegations above as if fully set forth herein.

146. Plaintiff and Class members were required to provide their PII to Defendant as a condition of being employed by Defendant.

147. Plaintiff and Class members provided their PII to Defendant in exchange for Defendant's services or employment. In exchange for the Private Information, Defendant promised to protect their PII from unauthorized disclosure.

148. On information and belief, Defendant promised to comply with industry standards and to make sure that Plaintiff's and Class members' Private Information would remain protected.

149. When Plaintiff and Class members provided their Private Information to Defendant as a condition of their relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

150. Implicit in the agreement between Plaintiff and Class members and Defendant to provide Private Information, was Defendant's obligation to:

a. Use such Private Information for business purposes only;

b. Take reasonable steps to safeguard that Private Information;

c. Prevent unauthorized disclosures of the Private Information;

d. Provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information;

e. Reasonably safeguard and protect the Private Information of Plaintiff and Class members from unauthorized disclosure or uses; and

f. Retain the Private Information only under conditions that kept such information secure and confidential.

151. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

152. By providing their sensitive data to Defendant's business customers, Class members entered into an implied contract with the reasonable expectation that Defendants, as custodian of this information, would take adequate measures to protect it. The collection and storage of such highly sensitive information necessarily carries with it a duty to implement reasonable security safeguards, consistent with industry standards and legal obligations. Defendant's failure to prevent the Data Breach constitutes a breach of this implied contractual obligation, directly harming Plaintiff and the Class, who reasonably relied on Defendant's promises and practices to keep their information secure.

153. Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

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

155. Defendant breached its implied contracts with Plaintiff and Class members by failing to safeguard and protect their Private Information.

156. As a direct and proximate result of Defendant's breach of the implied contracts, Class members sustained damages as alleged herein.

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

158. Plaintiff and Class members are also entitled to nominal damages for the breach of implied contract.

159. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to ***all*** Class members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

160. Plaintiff incorporates by reference the allegations above as if fully set forth herein.

161. Plaintiff and Class members conferred a monetary benefit on Defendant in the form of the provision of their Private Information, which Defendant accepted. Defendant would be unable to engage in its regular course of business without employees' Private Information.

162. Acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits 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 their own profits over the requisite data security.

163. Defendant has been unjustly enriched as a result of its failure to adequately safeguard the sensitive personal and medical information entrusted to them. Defendant retained the benefits of this data in the form of revenue and value derived from its business operations, while shifting the risk and costs of the resulting Data Breach, including identity theft risk, credit

monitoring, and loss of privacy, onto Plaintiff and the Class. Defendant's retention of these benefits without appropriate compensation to Class members is inequitable and unjust.

164. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures.

165. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

166. If Plaintiff and Class members knew that Defendant had not secured their Private Information adequately, they would not have agreed to provide their Private Information to Defendant.

167. Plaintiff and Class members have no adequate remedy at law.

168. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered or will suffer injury, including but not limited to:

a. Actual identity theft;

b. The loss of the opportunity to decide how their Private Information is used;

c. The compromise, publication, and/or theft of their Private Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;

e. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

f. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; and

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

169. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

170. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

171. Plaintiff incorporates by reference the allegations above as if fully set forth herein.

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

173. An actual controversy has arisen in the wake of Defendant's Data Breach regarding their present and prospective common law and other duties to reasonably safeguard their employees' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information.

174. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

175. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (i) that Defendant continues to owe a legal duty to secure former and current employees' Private Information and to timely notify former and current employees of a data breach under the common law, Section 5 of the FTCA, and various state statutes; and (ii) that Defendant continue to breach this legal duty by failing to employ reasonable measures to secure former and current employees' Private Information.

176. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect former and current employees' Private Information.

177. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at the Washington Post. The risk of another such breach is real, immediate, and substantial. If another breach at the Washington Post occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

178. The hardship to Plaintiff and Class members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at the Washington Post, Plaintiff and Class members will likely be subjected to fraud, identity theft, and other harm described herein. On the other hand, the cost to Defendant of

complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

179. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at the Washington Post, thus eliminating the additional injuries that would result to Plaintiff and the former and current employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. An Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff and Class members;

C. Equitable relief compelling Defendant to utilize appropriate methods and policies with respect to former and current employee data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. Equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Declaratory relief as requested;

F. Injunctive relief ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

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

H. An award of attorneys' fees and costs, and any other expense, including expert witness fees;

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

J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Date: December 4, 2025

Respectfully submitted,

Jane N. Manwarring
jmanwarring@classlawdc.com
Jason S. Rathod
jrathod@classlawdc.com
Nicholas A. Migliaccio
nmigliaccio@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

Counsel for Plaintiff