UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: WORKWAVE DATA BREACH LITIGATION	Case No.: 3:24-cv-10592-RK-JBD **CONSOLIDATED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs John Kratochwill and Branden Rogers ("Plaintiffs"), individually and on behalf of all others similarly situated, and on behalf of the general public, brings this Class Action Complaint, against defendant WorkWave LLC d/b/a TEAM Software ("TEAM" or "Defendant") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused Plaintiffs and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. TEAM develops cloud-based financial, operations and workforce management solutions designed for janitorial and security contractors with a distributed workforce.

3. As part of its business, Defendant obtained and stored the personal information of Plaintiffs and Class members.

4. By taking possession and control of Plaintiffs' and Class members' personal information, Defendant assumed a duty to securely store and protect it.

5. Defendant breached this duty and betrayed the trust of Plaintiffs and Class members by failing to properly safeguard and protect their personal information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

6. On July 26, 2024, TEAM detected suspicious activity on its TEAM application, indicating a data breach. Based on a subsequent forensic investigation, TEAM determined that cybercriminals infiltrated its inadequately secured computer environment and thereby gained access to its data files (the "Data Breach"). The investigation further determined that, through this infiltration, cybercriminals potentially accessed and acquired files containing the sensitive personal information of approximately 99,525 individuals.[1]

7. The personally identifiable information ("PII") accessed by cybercriminals included, but is not limited to, names, Social Security numbers, and driver's license numbers (collectively, "Personal Information").[2]

[1] *See* TEAM's breach notification letter, accessible at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a7671d63-bec5-4044-87c9-8fb8a9ac7d2c.html.

[2] *Id.*

8. Defendant's misconduct – failing to implement adequate and reasonable measures to protect Plaintiffs' and Class members' Personal Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Personal Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiffs and Class members across the United States.

9. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals, for decades to come.

10. Plaintiffs bring this class action lawsuit to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or reasonable industry cybersecurity measures to protect Class members' Personal Information.

11. As a result of the Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiffs and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of

their lives, as Plaintiffs and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information.

12. Additionally, Plaintiffs and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

13. Plaintiffs bring this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

II. THE PARTIES

14. Plaintiff Kratochwill is a citizen and resident of Middleton, Wisconsin.

15. Plaintiff Rogers is a citizen and resident of Fort Wayne, Indiana.

16. Defendant is a New Jersey limited liability company with its principal place of business in Holmdel, New Jersey. Upon information and belief, Defendant has only one member, Marathon Acquisition, Inc., which has its principal place of business in New Jersey.

III. JURISDICTION AND VENUE

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

18. The Class Action Fairness Act (CAFA) confers diversity jurisdiction to a class action where (1) the "matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs," and (2) "*any* member of a class of Plaintiff is a citizen of a State different from *any* defendant." 28 U.S.C. § 1332(d)(2) (emphasis added).

19. Class Members, including Plaintiffs, are victims of the Data Breach and are domiciled across the United States.

20. By having at least one "member of a class of Plaintiffs [who] is a citizen of a State different from any defendant," diversity jurisdiction is conferred here, since the matter in controversy exceeds $5,000,000. *See* 28 U.S.C. § 1332(d)(2) (establishing that diversity jurisdiction is conferred where the amount in controversy exceeds $5,000,000 and where "*any* member of a [proposed] class of Plaintiff is a citizen of a State different from *any* defendant") (emphasis added).

21. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts this State.

22. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further proper in this District under 28 U.S.C. § 1391(b)(2) because a

substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. WorkWave LLC, d/b/a Team Software

23. TEAM is a limited liability company who "develop[s] market-leading financial, operations and workforce management solutions for service contractors with distributed workforces, with a special focus on the cleaning, security and facilities management industries in North America, Australia and the U.K. and Ireland."[3]

24. TEAM provides business management software to help organize operations, streamline accounting processes and provide profitability insight.[4]

25. As part of its business, Defendant receives, collects, and maintains the highly sensitive PII of its service contractors' current and former employees and/or customers. In doing so, Defendant implicitly promises to safeguard their PII.

26. After customers' and employees' PII is input into TEAM's business software, Defendant maintains the PII in its computer systems and/or software. On information and belief, Defendant maintains former employees and customers' PII for years after their relationship is terminated.

[3] *See* https://teamsoftware.com/about/
[4] *Id.*

27. In collecting and maintaining customers' and employees' PII, Defendant agreed it would safeguard the data in accordance with its internal policies as well as state law and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII.

28. Indeed, Defendant understood the importance of adequate cybersecurity measures, declaring in its Privacy Policy, "[w]e have implemented reasonable, risk-based technical and organizational measures designed to secure your Personal Information from accidental loss and from unauthorized access, use, alteration, and disclosure." [5]

29. The Privacy Policy also promises:

> WorkWave is responsible for the processing of personal data it receives, under the DPF, and subsequently transfers to a third party acting as an agent on its behalf. WorkWave complies with the DPF Principles for all onward transfers of personal data from the EU, UK and Switzerland, including the onward transfer liability provisions.
>
> * * *
>
> *We will at all times maintain reasonable and appropriate security controls to protect personal information of Client Personnel . . .*[6]

30. In addition, Defendant's website assures:

> WorkWave wants to assure customers the security of their information is our top priority.

[5] Privacy Policy, WorkWave LLC, https://www.workwave.com/privacy-policy/ (last visited December 30, 2024).
[6] *Id.* (emphasis added).

* * *

WorkWave's Diligence to Information Security:

- WorkWave employs robust security measures to safeguard customer data.
- WorkWave regularly reviews and updates our security protocols to stay ahead of potential threats.

* * *

WorkWave values customer trust and remains committed to ensuring the security and privacy of information.[7]

31. Defendant understood the need to protect its service contractor's customers' and employees' PII and prioritize its data security.

32. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect customers' and employees' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to customers' and employees' PII.

[7] https://workwave.my.site.com/hirebyworkwave/s/article/Information-Security-TEAM (last visited Jan. 17, 2025).

B. The Data Breach and Defendant's Belated Notice

33. On July 26, 2024, TEAM detected suspicious activity on its TEAM application, indicating a data breach.[8]

34. Based on a subsequent forensic investigation, TEAM determined that cybercriminals infiltrated its inadequately secured computer environment and thereby gained access to its data files. The investigation further determined that, through this infiltration, cybercriminals potentially accessed and acquired files containing the sensitive personal information of approximately 99,525 individuals.[9]

35. The PII accessed by cybercriminals included, but is not limited to, names, Social Security numbers, and driver's license numbers.[10]

36. Despite the sensitivity of the PII that was exposed, and the attendant consequences to affected individuals as a result of the exposure, Defendant failed to disclose the Data Breach for several weeks from the time of the Breach. This inexplicable delay further exacerbated the harms to Plaintiffs and Class members.

37. Based on the notice letter received by Plaintiffs, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiffs' Personal Information was stolen in the Data Breach.

---

[8] *See* TEAM's breach notification letter, accessible at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a7671d63-bec5-4044-87c9-8fb8a9ac7d2c.html.
[9] *Id.*
[10] *Id.*

38. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Personal Information, exfiltrated the Personal Information from Defendant's network, and has engaged in (and will continue to engage in) misuse of the Personal Information, including marketing and selling Plaintiffs' and Class members' Personal Information on the dark web.

39. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' Personal Information confidential and to protect such Personal Information from unauthorized access.

40. Nevertheless, Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for Plaintiffs and Class Members.

41. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

42. Similarly, based on the delayed discovery of the Data Breach, it is evident that the infiltrated network, that Defendant allowed to store Plaintiffs' Private Information, did not have sufficiently effective endpoint detection.

43. Further, the fact that PII was acquired in the Data Breach demonstrates that the PII contained in the Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

44. Plaintiffs and Class Members entrusted Defendant with sensitive and confidential information, including their PII, which includes information (such as Social Security numbers) that are static, do not change, and can be used to commit a myriad of financial crimes.

45. The stolen Personal Information at issue has great value to the hackers.

C. Plaintiffs' Experiences

Plaintiff Kratochwill

46. Plaintiff Kratochwill provided his sensitive Personal Information to his employer who contracts with Defendant. Upon information and belief, Defendant thereafter acquired this Personal Information and used it when providing business services/software.

47. Plaintiff Kratochwill received a notice letter from Defendant dated November 12, 2024, informing him that his Personal Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

48. Plaintiff Kratochwill is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Personal Information exposed in any other data breach.

49. Plaintiff Kratochwill stores any documents containing his Personal Information in a safe and secure location. Plaintiff Kratochwill has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

50. Because of the Data Breach, Plaintiff Kratochwill's Personal Information is now in the hands of cybercriminals.

51. Plaintiff Kratochwill has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

52. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Kratochwill is now imminently at risk of crippling future identity theft and fraud.

53. Since the Data Breach, Plaintiff Kratochwill has experienced identity theft and fraud. Specifically, in the fall of 2024, Plaintiff Kratochwill experienced fraudulent purchases on his financial account. In addition, Plaintiff Kratochwill was notified that this Personal Information has been located on the dark web following the Data Breach. Furthermore, Plaintiff Kratochwill has experienced a significant increase in spam calls and texts in the past few months. Plaintiff Kratochwill

attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that he has never experienced anything like this prior to now.

54. As a result of the Data Breach, Plaintiff Kratochwill has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Kratochwill has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements, monitoring financial activity on a regular basis, checking his credit scores, addressing the fraudulent transactions, screening the influx of spam calls and texts, and taking other protective and ameliorative steps in response to the Data Breach.

55. The letter Plaintiff Kratochwill received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised to "remain vigilant by reviewing your account statements and credit reports closely."[11] In addition, the breach notification letter listed several "steps" that victims of the Data Breach should

[11] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a7671d63-bec5-4044-87c9-8fb8a9ac7d2c.html

take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[12]

56. As a result of the Data Breach, Plaintiff Kratochwill has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. Plaintiff Kratochwill fears that criminals will use his information to commit identity theft.

57. Plaintiff Kratochwill anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

58. Plaintiff Kratochwill has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Kratochwill's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Kratochwill's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Kratochwill's Personal

[12] *Id.*

Information; and (e) continued risk to Plaintiff Kratochwill's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

Plaintiff Rogers

59. Plaintiff Rogers provided his sensitive Personal Information to his employer who contracts with Defendant. Upon information and belief, Defendant thereafter acquired this Personal Information and used it when providing business services/software.

60. Plaintiff Rogers received a notice letter from Defendant dated November 12, 2024, informing him that his Personal Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

61. Plaintiff Rogers is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Personal Information exposed in any other data breach.

62. Plaintiff Rogers stores any documents containing his Personal Information in a safe and secure location. Plaintiff Rogers has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

63. Because of the Data Breach, Plaintiff Rogers's Personal Information is now in the hands of cybercriminals.

64. Plaintiff Rogers has suffered actual injury from the exposure and theft of his Personal Information—which violates his right to privacy.

65. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Rogers is now imminently at risk of crippling future identity theft and fraud.

66. Since the Data Breach, Plaintiff Rogers has received notification that his Personal Information has been located on the dark web. Plaintiff Rogers has also noticed a considerable increase in spam calls and texts in the months following the Data Breach. Plaintiff Rogers attributes the foregoing suspicious activity to the Data Breach given the time proximity, and the fact that this activity is highly unusual.

67. As a result of the Data Breach, Plaintiff Rogers has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Rogers has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements, addressing the increase in spam calls and texts, and taking other protective and ameliorative steps in response to the Data Breach.

68. The letter Plaintiff Rogers received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised to "remain vigilant by reviewing your account statements and credit reports closely."[13] In addition, the breach notification letter listed several "steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[14]

69. As a result of the Data Breach, Plaintiff Rogers has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Personal Information. Plaintiff Rogers fears that criminals will use his information to commit identity theft.

70. Plaintiff Rogers anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

71. Plaintiff Rogers has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Rogers's Personal Information being placed in

[13] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a7671d63-bec5-4044-87c9-8fb8a9ac7d2c.html
[14] *Id.*

the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Rogers's Personal Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Rogers's Personal Information; and (e) continued risk to Plaintiff Rogers's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

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

72. Defendant also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. Defendant is further required by various states' laws and regulations to protect Plaintiffs' and Class members' Personal Information.

74. Defendant owed a duty to Plaintiffs and the Class to design, maintain, and test its computer and application systems to ensure that the Personal Information in its possession was adequately secured and protected.

75. Defendant owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees (and others who accessed Personal Information within its computer systems) on how to adequately protect Personal Information.

76. Defendant owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on its systems in a timely manner.

77. Defendant owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

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

79. Defendant owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

80. Defendant owed a duty of care to Plaintiffs and the Class because it was a foreseeable victim of a data breach.

E. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

81. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[15] Yahoo,[16] Marriott International,[17] Chipotle, Chili's, Arby's,[18] and others.[19]

82. Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Personal Information that it collected and maintained.

83. Defendant was also on notice of the importance of data encryption of Personal Information. Defendant knew it kept Personal Information in its systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

---

[15] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[16] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[17] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[18] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[19] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

F. Cyber Criminals Will Use Plaintiffs' and Class Members' Personal Information to Defraud Them

84. Plaintiffs and Class members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class members and to profit off their misfortune.

85. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[20] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[21] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

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

[21] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

86. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[22]

87. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

This is exacerbated by the fact that the problems arising from a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

[23] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

> and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[24]

88. A particularly troublesome example of this effect is the development of "Fullz" packages. A "Fullz" package is a dossier of information that cybercriminals and other unauthorized parties can assemble by cross-referencing the Private Information compromised in a given data breach to publicly available data or data compromised in other data breaches. Automated programs can and are routinely used to create these dossiers and they typically represent an alarmingly accurate and complete profile of a given individual.

89. Therefore, through the use of these "Fullz" packages, stolen Private Information from this Data Breach can be easily linked to Plaintiffs' and the proposed Class members' phone numbers, email addresses, and other sources and identifiers. Thus, even if certain information such as emails, phone numbers, or credit card or financial accounts were not compromised in this Data Breach, criminals can easily create a Fullz package to use for identity theft, to commit fraudulent account activity on Plaintiff's and the Class's financial accounts, or to sell for profit.

[24] *Id.*

90. Upon information and belief, this has already transpired (and will continue to transpire) for Plaintiffs and the Class.

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

92. This data demands a much higher price on the black market. Martin W alter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[25]

93. This was a financially motivated Data Breach, as apparent from the targeted nature of the infiltration. The Personal Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

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

94. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[26]

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

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

96. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[28]

97. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

---

[26] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[27] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

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

98. Victims of the Data Breach, like Plaintiffs and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[29]

99. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

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

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

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

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

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

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

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

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

101. Moreover, Plaintiffs and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiffs' and Class members' Personal Information.

102. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiffs and all Class members will need to have identity theft monitoring protection for the rest of their lives.

103. None of this should have happened. The Data Breach was preventable.

G. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Personal Information

104. Data breaches are preventable.[30] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that

[30]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[31] she added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[32]

105. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[33]

106. 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.

107. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer

[31] *Id.* at 17.

[32] *Id.* at 28.

[33] *Id.*

needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.7 The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack 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.[34]

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

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

[34] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

these actions further clarify the measures businesses must take to meet their data security obligations.

110. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

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

112. Upon information and belief, Frontier failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Personal Information, resulting in the Data Breach.

113. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiffs' and Class Members' Personal Information.

114. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiffs' and Class members' Personal Information.

115. Defendant was at all times fully aware of its obligation to protect the Personal Information of Plaintiffs and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

116. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

117. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if Plaintiffs' and Class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach.

118. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps

to secure Plaintiffs' and Class members' Personal Information from those risks left that information in a dangerous condition.

119. Defendant disregarded the rights of Plaintiffs and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

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

121. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose Personal Information was compromised as a result of the Data Breach, including all persons who received breach notification letters.

122. Plaintiffs reserve the right to amend the above definition or to propose

subclasses in subsequent pleadings and motions for class certification.

123. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

124. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable.

125. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

126. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class that Plaintiffs seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

127. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the

burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

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

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiffs' and Class members'

Personal Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiffs and the Class to use reasonable care in protecting their Personal Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

i. Whether Defendant continues to breach duties to Plaintiffs and the Class;

j. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class and the general public;

m. Whether Defendant's actions alleged herein constitute gross negligence; and

n. Whether Plaintiffs and Class members are entitled to punitive damages.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

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

130. Defendant solicited, gathered, and stored the Personal Information of Plaintiffs and the Class as part of the operation of its business and in order to gain revenues.

131. Upon accepting and storing the Personal Information of Plaintiffs and Class members, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

132. Defendant had full knowledge of the sensitivity of the Personal Information, the types of harm that Plaintiffs and Class members could and would suffer if the Personal Information was wrongfully disclosed, and the importance of adequate security.

133. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiffs and the Class members had no ability to protect their Personal Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

134. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal information.

135. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to

Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

136. Defendant's duty extended to protecting Plaintiffs 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 also have recognized the existence of a specific duty to reasonably safeguard personal information.

137. Defendant had duties to protect and safeguard the Personal Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Personal Information. Additional duties that Defendant owed Plaintiffs and the Class include:

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

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

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

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

138. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal Information that Plaintiffs and the Class had entrusted to it.

139. Defendant breached its duty of care by failing to adequately protect Plaintiffs' and Class members' Personal Information. Defendant breached its duties by, among other things:

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

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

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

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

f. Failing to adequately train its employees to not store Personal Information longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's Personal Information;

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

i. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their Personal Information.

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

141. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

142. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Personal Information of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal Information of Plaintiffs and Class members while it was within Defendant's possession and control.

143. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps toward securing their Personal Information and mitigating damages.

144. As a result of the Data Breach, Plaintiffs 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 fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

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

146. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

147. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

148. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiffs' and Class members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiffs therefore are entitled to the evidentiary presumptions for negligence *per se*.

149. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiffs and the Class.

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

151. Defendant gathered and stored the Personal Information of Plaintiffs and the Class as part of its business, which affect commerce.

152. Defendant violated the FTC Act by failing to use reasonable measures to protect the Personal Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

153. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class members' Personal Information, and by failing to provide prompt and specific notice without reasonable delay.

154. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

155. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

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

157. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

158. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

159. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence.

160. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

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

162. Defendant entered into contracts with its clients to provide software and other services. As a material part of those contracts Defendant agreed to implement reasonable data security practices and procedures sufficient to safeguard the PII provided to it by its clients.

163. In its written policies, Defendant expressly and impliedly promised to Plaintiffs and Class Members that it would maintain the Personal Information it collects safe and secure.

164. For example, Defendant's Privacy Policy promises:

> WorkWave is responsible for the processing of personal data it receives, under the DPF, and subsequently transfers to a third party

> acting as an agent on its behalf. WorkWave complies with the DPF Principles for all onward transfers of personal data from the EU, UK and Switzerland, including the onward transfer liability provisions.
>
> * * *
>
> *We will at all times maintain reasonable and appropriate security controls to protect personal information of Client Personnel . . .*[35]

165. In addition, Defendant's website assures:

> WorkWave wants to assure customers *the security of their information is our top priority.*
>
> * * *
>
> **WorkWave's Diligence to Information Security:**
>
> - *WorkWave employs robust security measures to safeguard customer data.*
> - *WorkWave regularly reviews and updates our security protocols to stay ahead of potential threats.*
>
> * * *
>
> WorkWave values customer trust and remains committed to ensuring the security and privacy of information.[36]

166. These contracts were made for the benefit of Plaintiffs and the Class, as it was their confidential information that TEAM agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Personal

[35] *Id.* (emphasis added).
[36] https://workwave.my.site.com/hirebyworkwave/s/article/Information-Security-TEAM (last visited Jan. 17, 2025) (emphasis added).

Information belonging to Plaintiffs and the Class were the direct and primary objective of the contracting parties.

167. TEAM knew that if it were to breach these contracts with its staffing and financial clients, their consumers, including Plaintiffs and the Class, would be harmed by, among other things, fraudulent misuse of their Personal Information.

168. Defendant breached its contracts when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' PII.

169. As a reasonably foreseeable result of the breach, Plaintiffs and the Class were harmed by TEAM's failure to use reasonable data security measures to store their Personal Information, including but not limited to, the actual harm sustained from the loss of their Personal Information to cybercriminals.

170. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

VII. PRAYER FOR RELIEF

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

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing

the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

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

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

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

v. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

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

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

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

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach

when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

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

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

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

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

DATED: January 27, 2025

/s/ David J. DiSabato

David J. DiSabato
SIRI & GLIMSTAD LLP
745 Fifth Ave Suite 500
New York, NY 10151
T: (973) 273-3570

E: ddisabato@sirillp.com

A. Brooke Murphy
(admitted *pro hac vice*)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

David K. Lietz
(admitted *Pro Hac Vice)*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on January 27, 2025, the foregoing was filed electronically with the Clerk of Court using the CM/ECF System and was thereby served on all counsel of record.

/s/ David J. DiSabato
David J. DiSabato

ClassAction.org
