IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

ALISSA NEUFELD, individually and on behalf of all others similarly situated, Plaintiff, vs. TRIONFO SOLUTIONS, LLC and GALLAGHER BENEFIT SERVICES, INC., Defendants.	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMAND**

Plaintiff, Alissa Neufeld ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Trionfo Solutions, LLC ("Trionfo") and Defendant Gallagher Benefit Services, Inc. ("Gallagher:) (collectively, "Defendants"), to obtain damages, restitution, and injunctive relief for the putative class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a massive cyber-attack on Trionfo's computer systems between December 4, 2023, and December 6, 2023 ("Data Breach").

2. Trionfo is a technology company based in Itasca, Illinois, that creates software for the insurance industry, including programs that generate quotes, compare plans, and enable the easy management of employee benefits.

3. Gallagher is "a premier employee benefits and human resources consulting and actuarial firm."[1]

4. Trionfo maintains sensitive information in connection with certain insurance related services that it provides to Gallagher in connection with employer sponsored benefits.

5. In providing these services, and in the ordinary course of its business, Trionfo acquires, possesses, and analyzes sensitive personal information provided by the business customers, including Gallagher's. The information the business customers provide is information obtained from the business customers' employees, and in some circumstances, the information obtained is employee information from the customers of the business customers.

6. Information stolen in the Data Breach included these individuals' sensitive personally identifiable information ("PII"), including, but not limited to, names, addresses, dates of birth, Social Security numbers, telephone numbers and/or email addresses.

7. Plaintiff and Class Members are nationwide consumers who provided their PII directly to Trionfo's customers who then shared the information with Trionfo during the regular course of business.

8. Plaintiff and Class Members reasonably expected their PII would remain private and confidential, whither the information was provided directly or indirectly to the Defendants.

9. By acquiring and utilizing and benefiting from the PII for its business purposes, Trionfo owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiffs and Class Members. These duties required Trionfo to design and implement adequate data security systems to protect Plaintiffs and Class Members' PII in its possession and to keep the

[1] https://www.ncpers.org/gallagher-benefit-services

information confidential, safe, secure and protected from unauthorized disclosure, access, dissemination or theft.

10. Trionfo breached these duties by developing unsafe and unprotected access tools and implementing inadequate data security measures and protocols that failed to properly safeguard and protect Plaintiffs' and Class Members' PII from a foreseeable cyber-attack on its systems.

11. As a result, unauthorized actors gained access and exfiltrated and stole Plaintiffs' and Class Members' PII.

12. Currently, the full extent of the accessed and stolen PII, the scope of the Data Breach, and the root cause of the Data Breach are all known by and within the exclusive control of the Defendants, its agents, counsel, and forensic security vendors.

13. Trionfo breached its duties and obligations in one or more of the following ways: (1) designing, implementing, monitoring, and maintaining unreasonable and knowingly deficient safeguards against foreseeable threats; (2) designing, implementing, and maintaining unreasonable data retention policies; (3) insufficiently training staff on data security and data retention; (4) implementing security measures that did not comply with industry-standard data security practices; (5) omitting from its statements to Plaintiffs and Class Members information about Trionfo's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) implementing data security measures that were incapable of recognizing or detecting that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

14. Plaintiff and Class Members now face an ongoing and lifetime risk of identity theft, which is heightened by the exposure of their Social Security numbers to criminals.

15. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

16. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Trionfo's inadequate safeguarding of Class Members' PII that it 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.

17. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known and foreseeable risk to Defendants, and Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

18. In addition, Trionfo and its employees failed to properly monitor the computer network and systems that housed the PII. Had Trionfo properly monitored its property, it would have discovered the intrusion sooner.

19. Because of the Data Breach, Plaintiff and Class Members suffered injury and damages in the form of theft and misuse of their PII.

20. In addition, Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the PII that Defendants collected and maintained is now in the hands of data thieves.

21. Armed with the PII accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

22. As a further result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present 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.

23. Plaintiff and Class Members may also incur out of pocket costs for, for example, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

24. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

25. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed and/or removed from the network during the Data Breach.

26. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief--including improvements to Trionfo data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendants.

27. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct.

PARTIES

28. Plaintiff is a resident and citizen of Dallas, Texas. Plaintiff received a Notice Letter (defined below) dated May 22, 2024, from the Trionfo informing her that her PII was compromised and disclosed as a result of the Data Breach.

29. Defendant Trionfo is a limited liability company organized under the laws of the state of Illinois with its principal place of business located in Itasca, Illinois.

30. Defendant Gallagher is a corporation organized under the state laws of Delaware with its principal place of business located in Roling Meadows, Illinois.

JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the proposed Class, including Plaintiff, are citizens of states different from Defendants.

32. This Court has jurisdiction over Defendants through their business operations in this District, the specific nature of which occurs in this District. Defendants' principal place of businesses are in this District. Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

33. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendants' principal place of businesses are located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Defendants' Businesses

34. Trionfo is a technology company based in Itasca, Illinois, that creates software for the insurance industry, including programs that generate quotes, compare plans, and enable the easy management of employee benefits.

35. Gallagher is "a premier employee benefits and human resources consulting and actuarial firm."[2]

36. Plaintiff and Class Members are individuals who gave their PII to businesses that do business with Trionfo.

37. In the ordinary course and scope of its business, Trionfo contracts with companies, including Gallagher, who entrusted Defendants with the safeguarding of the PII belonging to their employees including that of the Plaintiff and the Class Members.

38. Defendants retain and store this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendants would be unable to perform its services.

[2] https://www.ncpers.org/gallagher-benefit-services

39. The information held by Trionfo's in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

40. By accepting and gaining control over Plaintiff's and Class Members' PII, Defendants promised to provide confidentiality and adequate security for this PII.

41. By obtaining, controlling, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

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

43. Plaintiff and the Class Members relied on Defendants 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

44. On or about January 9, 2024, Trionfo began notifying its business customers of the Data Breach. Surprisingly, neither Trionfo nor any of its business customers, including Gallagher, notified the Plaintiff for four months.

45. It was not until May 22, 2024, that Trionfo began sending Plaintiff and other Data Breach victims a Notice of Data Breach letter ("Notice Letter"), informing them that:

> **WHAT HAPPENED?**
> Trionfo learned that an unauthorized party gained access to certain Trionfo systems between December 4, 2023, and December 6, 2023. Upon discovering the incident, we promptly secured those systems and initiated an investigation. Based on the results of the investigation, we believe the unauthorized party may have acquired certain files from our systems.

WHAT INFORMATION WAS INVOLVED

Trionfo reviewed the contents of the files that may have been acquired and determined that they contained your name, address, date of birth, Social Security number, phone number and/or email address.[3]

46. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

47. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

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

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

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

Data Breaches Are Preventable

51. Trionfo could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

[3] The "Notice Letter".

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

53. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

54. To prevent and detect cyber-attacks and/or ransomware attacks, Trionfo could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

[4] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[5]

55. To prevent and detect cyber-attacks or ransomware attacks, Trionfo could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

[5] *Id.* at 3-4.

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[6]

56. Given that Trionfo was storing the PII of its clients' current and former customers and current and former employees, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

57. The occurrence of the Data Breach indicates that Trionfo failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of, upon information and belief, tens of thousands of individuals, including that of Plaintiff and Class Members.

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

[6] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Defendants Knew or Should Have Known of the Risk Because Companies in Possession of PII are Particularly Suspectable to Cyber-Attacks

59. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting companies that collect and store PII, like Defendants, preceding the date of the breach.

60. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

61. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[7]

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

63. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report

[7] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

64. Additionally, as companies became more dependent on computer systems to run their business,[9] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[10]

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

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

67. At all relevant times, Trionfoknew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Trionfo's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

68. Trionfowas, or should have been, fully aware of the unique type and the significant volume of data on Trionfo's server(s), amounting to, upon information and belief, thousands of

---

[8] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

[9] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[10] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

69. The injuries to Plaintiff and Class Members were directly and proximately caused by Trionfo's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

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

71. As company in possession of consumers' PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them by consumers on behalf of Plaintiff and Class Members and of the foreseeable consequences if its data security systems, or those on which it transferred PII, were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

72. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] 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

[11] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

73. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[13]

74. For example, PII can be sold at a price ranging from $40 to $200.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

75. Social Security numbers, which were compromised for some Class Members in the Data Breach, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by some Class Members, can lead to identity theft and extensive financial fraud:

> 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.[16]

76. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

---

[12] *Id.*

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

77. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

78. Based on the foregoing, 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—names, dates of birth, and Social Security numbers.

79. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[17]

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

81. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

[17] 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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

Defendants Fail to Comply with FTC Guidelines

82. The Federal Trade Commission ("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.

83. 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 consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to 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.

84. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be

[18] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

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.

85. The FTC has brought enforcement actions against businesses for failing to protect 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. These enforcement actions include actions against entertainment and employee benefit provider companies, like Defendants.

87. Defendants failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

88. Defendants were at all times fully aware of their obligation to protect the PII of its customers and employees. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Failed to Comply with Industry Standards

89. As noted above, experts studying cyber security routinely identify technology and employee benefit provider companies in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

90. Several best practices have been identified that a minimum should be implemented by technology and employee benefit provider companies in possession of PII, like Defendants, including but not limited to: educating all consumers; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which consumers can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard in the technology and employee benefit provider industries include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

92. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation 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 all established standards in reasonable cybersecurity readiness.

93. These foregoing frameworks are existing and applicable industry standards in the technology and employee benefit provider industries. Upon information and belief, Defendants

failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages

94. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk Of Identity Theft

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

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

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

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

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

100. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[19]

[19] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

101. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

102. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

103. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

104. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

105. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

106. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud.

Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

107. Thus, due to the actual and imminent risk of identity theft, Trionfo's Notice Letter instructs Plaintiff and Class Members to do the following: "this letter provides precautionary measures you can take to help protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant against incidents of identity theft and fraud and review your financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis."[20]

108. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach as well as monitoring their financial accounts and credit reports for fraudulent activity, which may take years to detect.

109. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

110. These efforts are also consistent with the steps that FTC recommends that data breach 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

[20] Notice Letter.

[21] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

111. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[23]

Diminution Value Of PII

112. PII is a valuable property right.[24] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

113. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[25]

114. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[26,27]

---

[22] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps
[23] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").
[24] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[25] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[26] https://datacoup.com/
[27] https://digi.me/what-is-digime/

115. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[28]

116. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[29]

117. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

118. Based on the foregoing, 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, e.g., names, dates of birth, and Social Security numbers.

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

120. The fraudulent activity resulting from the Data Breach may not come to light for years.

121. At all relevant times, Trionfo knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable

---

[28] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

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

consequences that would occur if Trionfo's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

122. Trionfo was, or should have been, fully aware of the unique type and the significant volume of data on Trionfo's network, amounting to, upon information and belief, tens of thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

123. The injuries to Plaintiff and Class Members were directly and proximately caused by Trionfo's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit & Identity Theft Monitoring is Reasonable and Necessary

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

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

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

127. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from the Data Breach.

Plaintiff's Experience

128. Plaintiff has and has had various insurance policies, some of which have bene procured in connection with her employment as a nurse. At some point, her employers or those in which they do business with, must have provided her PII to Defendants, in the ordinary course of obtaining insurance.

129. At the time of the Data Breach, Trionfo retained Plaintiff's' PII in its system.

130. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to anyone had she known it would be shared with Defendants who had lax security measures.

131. Plaintiff received the Notice Letter, by email, from Trionfo. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties.

132. As a result of the Data Breach, and at the direction of Trionfo's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach as well as monitoring her financial accounts and credit reports for fraudulent activity, which may take years to detect. Plaintiff has spent significant time on activities in response to the Data Breach—valuable time

Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

133. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

134. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

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

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

137. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

138. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

139. Plaintiff brings this action individually and on behalf of all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

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

> **Nationwide Class**
> All persons in the United States whose PII was maintained on Trionfo's computer systems that were compromised in the Data Breach including those who were sent Notice of Data Breach Incident emails from Trionfo ("Class").

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

142. Plaintiff reserves the right to amend the definitions of the Class and/or add a Class if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

143. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

144. Numerosity. The members of the Classes are so numerous that joinder of all of them is impracticable. Although the precise number is currently unknown to Plaintiff and exclusively in the possession of Defendants, upon information and belief, tens of thousands of individuals' PII was compromised in the Data Breach.

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

a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b) Whether Trionfo failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber-attack;

c) Whether Trionfo's data security systems prior to and during the cyber-attack complied with applicable data security laws and regulations;

d) Whether Trionfo's data security systems prior to and during the cyber-attack were consistent with industry standards;

e) Whether Defendants owed a duty to Class Members to safeguard their PII;

f) Whether Defendants breached its duty to Class Members to safeguard their PII;

g) Whether computer hackers obtained Class Members' PII in the cyber-attack;

h) Whether Trionfo 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 Defendants' misconduct;

j) Whether Defendants owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendants breached that duty;

k) Whether Defendants' conduct was negligent;

l) Whether Defendants' acts, inactions, and practices complained of herein amount to an invasion of privacy;

m) Whether Defendants' actions violated federal law; and

n) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

146. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the cyber-attack.

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

148. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' 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.

149. 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 that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendants. 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.

150. Defendants have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
Negligence
(On Behalf of Plaintiff and All Class Members)

151. Plaintiff realleges and incorporates herein paragraphs 1-150 above, as if fully set forth herein.

152. Defendants were entrusted with Plaintiff's and Class Member' PII on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

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

154. By collecting and storing this data on Trionfo's computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Trionfo's duty included a responsibility to implement processes by which it could detect a breach of their

security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

155. Defendants 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 their systems and networks, and the personnel responsible for them, adequately protected the PII.

156. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

157. Defendants' duty to use reasonable security measures required Defendants to reasonably protect confidential data from any intentional or unintentional use or disclosure. In addition,

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

159. Defendants' 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 Defendants are bound by industry standards to protect confidential PII.

160. Defendants breached their duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to have in place mitigation policies and procedures;

d. Allowing unauthorized access to Class Members' PII;

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

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

161. Defendants owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

162. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

163. Defendants further breached their duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact.

164. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Trionfo's inadequate security protocols.

165. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Trionfo's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

166. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act WAS intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statute intended to guard against.

167. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

168. 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.

169. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

170. It was foreseeable that Trionfo's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was

reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting companies in possession of PII

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

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

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

174. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

175. Defendants' 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.

176. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

177. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

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

179. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

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

181. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as

Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

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

183. Defendants' negligent conduct is ongoing, in that they still hold the PII of Plaintiff and Class Members in an unsafe and insecure manner.

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

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and All Class Members)

185. Plaintiff realleges and incorporates herein paragraphs 1-150 above, as if fully set forth herein.

186. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

187. Defendants' failure to comply with the FTC Act and similar state statutes and regulations constitutes negligence *per se.*

188. Plaintiff and Class Members are within the class of persons that the Federal Trade Commission Act intended to protect, and the type of harm that resulted from the Data Breach was the type of harm that the Federal Trade Commission Act intended to guard against.

189. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

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

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

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

192. Plaintiff realleges and incorporates herein paragraphs 1-150 above, as if fully set forth herein.

193. Upon information and belief, Trionfo funds its data security measures entirely from their general revenue, including payments made by Plaintiff and the Class Members.

194. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Trionfo.

195. Plaintiff and Class Members conferred a monetary benefit upon Defendants. Specifically, they provided Defendants with their PII. In exchange, Plaintiff and Class Members should have had their PII protected with adequate data security.

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

197. Defendants were enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid the data security obligations 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 Trionfo's failure to provide the requisite security.

198. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

199. Defendants acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

200. If Plaintiff and Class Members knew that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendants.

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

202. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of

benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

203. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

204. Defendants 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. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

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

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

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

xi. requiring Defendants to conduct regular database scanning and securing checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: June 4, 2024.

Respectfully Submitted,

/s/*Gary M. Klinger*

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Jeff Ostrow
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite. 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
ostrow@kolawyers.com

Attorneys for Plaintiff and the Putative Class

ClassAction.org