UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

TAMARA KIRTLEY, individually and on behalf all others similarly situated,	)	
Plaintiff,	)	**CASE NO._____**
v.	)	**CLASS ACTION**
STARTEK, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff, Tamara Kirtley, on behalf of herself and all others similarly situated, brings this action against Defendant STARTEK, INC. ("Startek" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from the Defendant. 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.

I. NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") that was perpetrated against Defendant STARTEK, a company that provides customer service to some of the largest companies in the world, which held in its possession certain personally identifiable information ("PII") of the Plaintiff and the putative Class Members, who are (or were) employees of Defendant. As a result of the Data Breach, Plaintiff and thousands of Class Members, suffered ascertainable losses in the form of the loss of the benefit of their bargain,

out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

3. The private information compromised in the Data Breach included names, Social Security numbers (the holy grail for identity thieves), and dates of birth (collectively, the "Private Information").

4. The Private Information compromised in the Data Breach was exfiltrated by the cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' Private Information.

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

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a

known risk to Defendant and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

9. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

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

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

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

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

14. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

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

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct.

II. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant because the conduct at issue in this case occurred, among other locations, in Colorado, where Defendant is headquartered.

19. Venue is proper because a substantial portion of the events complained of occurred in this District.

III. PARTIES

20. Plaintiff Tamara Kirtley is and at all times mentioned herein was an individual citizen of the State of Ohio, residing in the city of Cincinnati. Plaintiff Kirtley was an employee of Startek. As a condition of Plaintiff's employment at Startek, she was required to provide her PII to Defendant. Plaintiff received notice of the Data Breach on or about January 21, 2022. A copy of the notice she received is attached as Exhibit A (the "Notice Letter").

21. Defendant STARTEK is a Delaware corporation with its principal place of business at Carrara Place, 4th floor, Suite 485, 6200 South Syracuse Way, Greenwood Village, Colorado.

IV. STATEMENT OF FACTS

A. Nature of Defendant's Business.

22. Defendant is a customer experience management solutions provider. Defendant provides customer service to some of the largest companies in the world.

23. According to Defendant's website, Defendant helps its clients break down the complexity of their customer lifecycle and helps customers build and sustain emotional connections with its clients' brands.

24. Defendant boasts about using a "tech-enabled and human assisted digital solutions" to assist its clients with strengthening its customer relationships.

25. According to Defendant, it has "partnered with global brands for over 3 decades now —working with them across their consumer value chain and providing new age customer

experience solutions and insights that are helping them define and reach their target audiences with greater efficiency and better value for every dollar spent."

26. Defendant works across 46 locations in 13 countries, with over 40,000 employees managing almost half a billion customer interactions every year for over 150 clients in different industries.

27. On information and belief, in the course of collecting Private Information from employees, including Plaintiff, Startek promised to provide confidentiality and adequate security for employee data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

28. Startek made these promises in, among other things, its Notices of Privacy Practices that are distributed to employees in the course of the employment enrollment process.[1]

29. Plaintiff and the Class Members, as former and current Startek employees, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

30. In the course of their employment relationship, employees, including Plaintiff and Class Members, provided Startek with at least the following Private Information:

a. names;

b. dates of birth; and

---

[1] *See e.g.,* https://careers.startek.com/privacy-policy.

c. Social Security numbers.

31. Startek had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

B. The Data Breach.

32. On December 23, 2021 Defendant Startek determined that an unauthorized individual "gained access to and obtained data" the Startek computer network on June 26, 2021.[2]

33. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as an employer that collects, creates, and maintains PII.

34. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Startek that included the Private Information of Plaintiff and Class Members.

35. The files stolen from Startek contained at least the following information of Plaintiff and Class Members: first names, last names, dates of birth, and Social Security numbers.

36. The Private Information contained in Startek's network was not encrypted.

37. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff believes her stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals.

38. Incredibly, Startek admits in the Notice Letter that Plaintiff's Private Information was "accessed" and "acquired" by cybercriminals in the Data Breach.[3]

---

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/202bb844-5131-4615-acad-da66748b55e1.shtml

[3] *See* Exhibit A attached thereto.

39. As a result of the Data Breach, Startek is informing Plaintiff and Class Members to take steps to "protect your personal information" and also encouraging Class Members to enroll in credit monitoring and identity theft restoration services.[4]

40. That Startek is encouraging its employees and former employees to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

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

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

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

43. Startek acquires, collects, and stores a massive amount of personally identifiable information ("PII") on its employees, former employees and other personnel.

44. As a condition of employment, or as a condition of receiving certain benefits, Startek requires that employees, former employees and other personnel entrust it with highly sensitive personal information.

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

---

[4] *Id.*

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

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

The Ransomware Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

48. It is well known that PII, including social security numbers in particular, is an invaluable commodity and a frequent target of hackers.

49. Individuals place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

50. Individuals are particularly concerned with protecting the privacy of their Social Security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

51. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[5]

52. 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

[5] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

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), Startek knew or should have known that its electronic records would be targeted by cybercriminals.

53. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

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

At All Relevant Times Startek Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

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

56. Startek's duty to use reasonable security measures arose as a result of the special relationship that existed between Startek, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted Startek with their PII as a condition of their employment with Startek.

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

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

a. Maintaining a secure firewall configuration;

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

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

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

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[6] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[7]

---

[6] 17 C.F.R. § 248.201 (2013).

[7] *Id*.

60. The ramifications of Startek's failure to keep its consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims may continue for years.

The Value of Personal Identifiable Information

61. The PII of consumers 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. For example, personal information can be sold at a price ranging from $40 to $200.[8]

62. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[9]

63. Social Security numbers, for example, are among the worst kind of personal information 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 is the case here, 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.[10]

---

[8] *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/.

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

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

64. 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 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.

65. Even then, a new Social Security number may not be effective, as "[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."[11]

66. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[12]

67. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[13]

68. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals

---

[11] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

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

[13] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

69. The information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

70. To date, Startek has offered its consumers only one year of identity monitoring service. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

71. The injuries to Plaintiff and Class Members were directly and proximately caused by Startek's failure to implement or maintain adequate data security measures for its current and former customers.

Startek Failed to Comply with FTC Guidelines

72. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

73. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[15] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is

[14] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[15] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

74. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[16]

75. The FTC recommends that businesses:

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

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

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

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

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

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

---

[16] FTC, *Start With Security*, *supra* note 18.

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

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

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

76. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the 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.

77. Because Class Members entrusted Startek with their PII, Startek had, and has, a duty to the Class Members to keep their PII secure.

78. Plaintiff and the other Class Members reasonably expected that when they provide PII to Startek, Startek would safeguard their PII.

79. Startek was at all times fully aware of its obligation to protect the personal and financial data of employees, including Plaintiff and members of the Class. Startek was also aware of the significant repercussions if it failed to do so.

80. Startek's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' Social Security numbers, driver's license numbers, financial account information, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed.

81. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers, financial account information and driver's license numbers.

82. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to employment with Defendant, Plaintiff and other reasonable former and current employees understood and expected that, as part of that employment relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

83. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

84. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

85. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

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

87. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[17]

88. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and

[17] *Id.*

continuing increased risk of identity theft and identity fraud.[18] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[19] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[20] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

89. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

90. Defendant openly admits that the cybercriminals "acquired" and "obtained" Plaintiff's and Class Members' data in the Breach.

Plaintiff Kirtley's Experience

91. Prior to the Data Breach Plaintiff Kirtley was employed at Startek. In the course of enrolling in employment with Startek and as a condition of employment, she was required to supply Startek with her PII, including but not limited to her name, address, date of birth, and Social Security number.

92. Plaintiff received the *Notice of Data Breach*, in January of 2022.

93. Plaintiff has experienced an increase in the number of spam phone calls, emails and texts since the Data Breach, which appear to be placed with the intent of obtaining personal

---

[18] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.

[19] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.

[20] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

information to commit identity theft by way of a social engineering attack. As a result, Plaintiff Kirtley was required to spend time obtaining a credit report and monitoring her credit history and financial accounts for suspicious activity.

94. In response to the Notice of Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which included and will include time spent verifying the legitimacy of the *Notice of Data Breach*, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

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

96. Plaintiff stores any and all documents containing PII in a safe and secure location and shreds any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

97. Plaintiff suffered actual injury and damages as a result of the Data Breach. Implied in her employment contract with Startek was the requirement that it adequately safeguard her PII. Plaintiff would not have worked for Startek had Startek disclosed that it lacked data security practices adequate to safeguard PII.

98. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that she entrusted to Startek for the purpose of employment, which was compromised by the Data Breach.

99. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially her Social Security number.

100. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

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

V. CLASS ACTION ALLEGATIONS

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

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

> All persons whose Private Information was maintained on Defendant Startek's computer systems that were compromised in the Data Breach, and who were sent Notice of the Data Breach.

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

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

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

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

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

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

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

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

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

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

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant's acts, inactions, and practices complained of herein violated the Colorado data protection laws invoked below;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiff and All Class Members)

115. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 114 above as if fully set forth herein.

116. Defendant required Plaintiff and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits.

117. Plaintiff and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information.

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

119. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

120. Defendant 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.

121. Defendant had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Colo. Rev. Stat. § 6-1-713.5.

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

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

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

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

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII; and

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

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

125. 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.

126. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

127. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

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

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

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

130. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 114 above as if fully set forth herein.

131. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their employment with Defendant.

132. Plaintiff and Class Members provided their labor to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure.

133. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

134. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

135. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access

and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

136. When Plaintiff and Class Members provided their PII to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

137. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

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

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

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

141. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

142. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

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

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

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

146. Plaintiff restates and realleges paragraphs 1 through 114 above as if fully set forth herein.

147. Plaintiff alleges Count III (unjust enrichment) solely in the alternative to Count II (breach of implied contract).

148. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their labor, and Defendant.

149. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

150. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof.

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

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

152. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

155. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how

to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

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

158. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 114 above as if fully set forth herein.

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

160. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

161. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect employee PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

162. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

163. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

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

165. In addition, Defendant's conduct violated Colo. Rev. Stat. § 6-1-713.5. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

166. Defendant failed to comply with Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiff's PII but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that

data breaches—especially health data—were on the rise, and that medical institutions were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

167. Plaintiff and Class Members are within the class of persons that Colo. Rev. Stat. § 6-1-713.5 was intended to protect.

168. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

169. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

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

171. As a direct and proximate result of Defendant's 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.

FIFTH COUNT
Invasion of Privacy by Intrusion
(On Behalf of Plaintiff and All Class Members)

172. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 114 as if fully set forth herein.

173. The State of Colorado recognizes the tort of Invasion of Privacy by Intrusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

174. Plaintiff and the Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

175. By intentionally failing to keep Plaintiff's and the Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by intrusion.

176. Defendant knew that ordinary persons in Plaintiff's or the Class Members' positions would consider this an invasion of privacy and Defendant's intentional actions highly offensive and objectionable.

177. Defendant invaded Plaintiff's and the Class Members' right to privacy and intruded into Plaintiff's and the Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

178. Defendant intentionally concealed from Plaintiff and the Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

179. In failing to protect Plaintiff's and the Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and the Class Members' rights to have such information kept confidential and private.

180. Plaintiff and the Class Members sustained damages (as outline above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

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

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

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

e. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: January 28, 2022

Respectfully submitted,

/s/ *Gary M. Klinger*
Gary M. Klinger
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
Email: gklinger@masonllp.com

Gary E. Mason
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dlietz@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Customer Service Co. StarTek Facing Class Action Over Employee Data Breach

---