IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JEANINE KEEYS, individually and on behalf of all others similarly situated, Plaintiff, v. TRC STAFFING SERVICES, INC. d/b/a TRC TALENT SOLUTIONS, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jeanine Keeys ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant TRC Staffing Services, Inc. d/b/a TRC Talent Solutions. ("Defendant" or "TRC"), and alleges as follows:

JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367 because

they form part of the same case or controversy as the claims within the Court's original jurisdiction.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiff's claims arise out of Defendant's contacts with this district.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

PARTIES

4. Plaintiff Jeanine Keeys is a resident and citizen of North Carolina.

5. Defendant TRC is a Georgia corporation with its principal place of business located at 5909 Peachtree Dunwoody Road, Suite D-1100, Atlanta, Georgia 30328.

FACTUAL ALLEGATIONS

TRC

6. Defendant TRC represents that it is "full-service talent solutions provider" and "staffing firm[]"[1] that "leverage[es] more than 40 years of workforce

[1] *See* https://www.linkedin.com/company/trc-talent-solutions (last accessed June 12, 2024).

best practices and results across more than 15 different industries [to] create the solutions businesses need."[2]

7. Defendant's Privacy Policy represents that it places significance upon protecting the information provided to it by third parties, informing them that, "[y]our privacy matters to us."[3]

8. TRC's Privacy Policy further represents that:

> We maintain robust technological and organizational security measures to safeguard your personal information. These measures are designed to prevent accidental loss, unauthorized access, alteration, destruction, or disclosure of your data. Our policy ensures that only individuals with a legitimate business need have access to your personal information. Those handling your data adhere to TRC's IT Information and Security rules, data protection guidelines, and other internal policies.[4]

9. Plaintiff and Class members are employees of Defendant.

10. Plaintiff and Class members provided certain Personally Identifying Information ("PII") to Defendant.

11. As a sophisticated staffing services company with an acute interest in maintaining the confidentiality of the PII entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII in its possession.

---

[2] *See* https://trctalent.com/about/ (last accessed June 12, 2024).
[3] *See* https://trctalent.com/privacy-policy/ (last accessed June 12, 2024).
[4] *Id.*

The Data Breach

12. According to Defendant, on April 12, 2024, Defendant "identified suspicious activity on certain computer systems that included the encryption of certain files."[5]

13. Defendant claims that it "took steps to secure its environment and to launch an investigation into the nature and scope of the activity." Defendant's investigation yielded the discovery that "an unknown actor gained access to certain systems between March 25, 2024 and April 12, 2024, and may have accessed or acquired information from these systems," which included Plaintiff's and the Class's PII (the "Data Breach").[6]

14. Defendant claims to have identified Plaintiff and Class members as individuals whose PII was potentially accessed by an unauthorized actor on May 9, 2024.[7]

15. The compromised data includes affected persons' full names and Social Security numbers. [8]

[5] *See* Data Breach Notification Letter, attached hereto as Exhibit 1.
[6] *Id.*
[7] *Id.*
[8] *Id.*

16. According to a notice of data breach filed with the Attorney General of Maine, the Data Breach has affected 158,593 individuals.[9]

17. Defendant began notifying affected persons on May 24, 2024.[10]

18. Defendant's letter offered free credit monitoring services to those potentially impacted by the breach.

19. Defendant's letter provided those potentially affected by the Data Breach with a document outlining "Steps [They] Can Take to Help Protect Personal Information."[11]

20. Defendant did not state why it was unable to prevent the Data Breach or which security feature failed.

21. Defendant did not state why it did not identify individuals whose PII was compromised until nearly one month after discovering the breach.

22. Defendant did not state why it did not contact potentially affected individuals about the Breach until two weeks after they were identified.

23. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

---

[9] *See* Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a.shtml

[10] *Id.*

[11] *See* Exhibit 1.

Injuries to Plaintiff and the Class

24. On or around May 24, 2024, Plaintiff received a breach notification from Defendant indicating that her PII "may" have been compromised during the Data Breach.[12] According to the notification letter, the Data Breach may have exposed Plaintiff's name and Social Security number.

25. After the Data Breach, Plaintiff has received a significant increase in phishing emails and/or spam calls daily, to the point that she has disabled her voice mail.

26. In response to the Data Breach, Plaintiff has spent significantly more time checking her bank and credit card statements than she did prior to the Data Breach.

27. Plaintiff is very concerned about the theft of her PII and has and will continue to spend substantial amounts of time and energy monitoring her credit status.

28. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff's PII, Plaintiff and the Class have been damaged.

29. Plaintiff and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring

[12] *Id.*

accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

30. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[13]

31. In addition to fraudulent charges and damage to their credit, Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j)

[13] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

paying late fees and declined payment penalties as a result of failed automatic payments.

32. Plaintiff and the Class have suffered severe emotional distress as a result of their PII being compromised and will continue to suffer for an indefinite period of time. Since Plaintiff and the Class may not change their Social Security numbers, their heightened risk of becoming victims of fraud is now permanent. Plaintiff and the Class will remain aware of both this permanent risk as well as their permanent inability to cure that risk until it manifests itself in the form of fraud.

33. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value and/or use of their PII entrusted to Defendant, and loss of privacy.

The Value of PII

34. It is well known that PII, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

35. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[14]

[14] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study*

36. People 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.[15]

37. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[16] 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."[17] The Social Security Administration's reactive security measures make Plaintiff and Class Members especially prone to

(Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[15] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[16] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[17] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

severe anxiety and emotional distress. Victims of a data breach must remain conscious of their vulnerability of identity theft, awaiting nefarious use of their social security information, while knowing they may not receive protection from that misuse until after it has occurred.

38. Defendant acknowledged the immense value of that PII had to Plaintiff and the Class insofar as it sent them a document outlining "Steps You Can Take To Help Protect Personal Information" and provided them with a year of credit monitoring services. However, the provision of credit monitoring services is abbreviated, and the document that guides Plaintiff and the Class in protecting their PII serves to emphasize that Defendant has placed the onus on those affected to retain the value of their PII.

Industry Standards for Data Security

39. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, and Capital One, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

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

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

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

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

41. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[18] and protection of PII[19] which includes basic security standards applicable to all types of businesses.

42. 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

[18] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[19] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

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.

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.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[20]

44. Because Defendant was entrusted with consumers' PII, it had, and has, a duty to consumers to keep their PII secure.

45. Consumers, such as Plaintiff and the Class, reasonably expect that when they provide PII to companies or when those companies forward their PII to companies such as Defendant, that their PII will be safeguarded.

46. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

CLASS ACTION ALLEGATIONS

47. Plaintiff, individually and on behalf of all others, brings this class action pursuant to Fed. R. Civ. P. 23.

48. The proposed Class are defined as follows:

> All persons whose PII was maintained on Defendant's servers and was compromised in the Data Breach.

[20] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

49. Plaintiff reserves the right to modify, change, or expand the definitions of the proposed Class based upon discovery and further investigation.

50. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, Defendant has reported that the number of persons affected by the Data Breach is 158,593 individuals.[21] The Class members can be readily identified through Defendant's records.

51. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

[21] *See* Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a.shtml

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class's PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class's PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

52. *Typicality*: The claims or defenses of Plaintiff are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

53. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiff has retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

54. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as whether Defendant owed a duty to Plaintiff and the Class

and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

55. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

56. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

57. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making

appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

58. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

59. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CAUSES OF ACTION

COUNT I
NEGLIGENCE/ NEGLIGENCE PER SE

60. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

61. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure to third parties, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that

Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII.

62. Defendant's duties to use reasonable data security measures also arose under Section 5 of the FTC 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 PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

63. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

64. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII.

65. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws

reasonable standards of care necessary to safeguard and protect Plaintiff's and Class members' PII within its possession, custody, and control.

66. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

67. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the breach.

68. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

69. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

70. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised.

71. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and the Class have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and the Class to the extent their PII has been diminished in value because Plaintiff and the Class no longer control their PII and to whom it is disseminated. Defendant is further liable to Plaintiff and the Class to the extent that they have suffered anxiety and emotional distress as a result of their heightened risk of becoming victims of credit fraud and identity theft.

COUNT II
INVASION OF PRIVACY

72. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

73. Plaintiff and Class members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

74. Defendant invaded Plaintiff's and the Class's right to privacy by allowing the unauthorized access to their PII and by negligently maintaining the confidentiality of Plaintiff's and the Class's PII, as set forth above.

75. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII was disclosed without prior written authorization from Plaintiff and the Class.

76. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class provided and disclosed their PII to Defendant privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

77. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class's PII was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class suffered damages as described herein.

78. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII with a willful and conscious disregard of their right to privacy.

79. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class severe and irreparable injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and the Class's PII with sub-standard and insufficient protections.

COUNT III
UNJUST ENRICHMENT

80. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

81. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

82. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on cybersecurity measures to secure Plaintiff's and the Class's PII.

83. Defendant also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

84. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead made a conscious and opportunistic calculation to increase its own profits at the expense of Plaintiff's and the Class's security. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiff and the Class. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

85. Plaintiff and the Class suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII, Plaintiff and the Class suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, increased risk of harm, and severe anxiety and emotional distress.

86. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and the Class, wherein it profited from interference with Plaintiff's and

the Class's legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

87. Accordingly, Plaintiff, on behalf of herself and the Class, respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII, and/or compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees, pursuant to O.C.G.A. § 13-6-11, or otherwise;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury.

Dated: June 19, 2024.

Respectfully submitted,

/s/ N. Nickolas Jackson
N. Nickolas Jackson
Georgia Bar No. 841433
J. Benjamin Finley
Georgia Bar No. 261504
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Phone: (404) 978-6971
Fax: (404) 320-9978
njackson@thefinleyfirm.com
bfinley@thefinleyfirm.com

Jeffrey S. Goldenberg
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Telephone: (513) 345-8291
jgoldenberg@gs-legal.com
(Pro hac vice to be filed)
Charles E. Schaffer
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: 215-592-1500
Fax: 215-592-4663
cschaffer@lfsblaw.com
(Pro hac vice to be filed)

Brett R. Cohen, Esq.
LEEDS BROWN LAW, P.C.
One Old Country Road - Suite 347

Carle Place, New York 11514
Phone: 516-874-4505
bcohen@leedsbrownlaw.com
(Pro hac vice to be filed)

Counsel for Plaintiff and Proposed Class

CERTIFICATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ N. Nickolas Jackson
N. Nickolas Jackson

JS44 (Rev. 10/2020 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

Jeanine Keeys

DEFENDANT(S)

TRC Staffing Services, Inc.

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF North Carolina
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Gwinnett
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

N. Nickolas Jackson
The Finley Firm, P.C.
3535 Piedmont Road, Bldg 14, Suite 230
Atlanta, Georgia 30305
404-320-9979
njackson@thefinleyfirm.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☑ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☑ 1	☐ 1	CITIZEN OF THIS STATE	☑ 4	☐ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☐ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. ORIGIN (PLACE AN "X "IN ONE BOX ONLY)

- ☑ 1 ORIGINAL PROCEEDING
- ☐ 2 REMOVED FROM STATE COURT
- ☐ 3 REMANDED FROM APPELLATE COURT
- ☐ 4 REINSTATED OR REOPENED
- ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

28 U.S.C. Section 1332(d)(2)(A). This is a class action filed by Plaintiff and all others similarly situated for Data Breach that happened due to Defendant's failure to safeguard Plainitff's protected personally identifiable information. Suit for damages and other relief for negligence and negligence per se resulting from data breach, declaratory and injunctive relief.

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____

(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☑ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK
- ☐ 880 DEFEND TRADE SECRETS ACT OF 2016 (DTSA)

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 485 TELEPHONE CONSUMER PROTECTION ACT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT 899
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** in excess of $5,000,000

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE Calvert **DOCKET NO.** 1:24-cv-02398

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)
- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☑ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

6/19/24

SIGNATURE OF ATTORNEY OF RECORD **DATE**