JASON R. HULL [11202]
JHULL@MOHTRIAL.COM
TREVOR C. LANG [14232]
TLANG@MOHTRIAL.COM
MARSHALL OLSON & HULL, PC
NEWHOUSE BUILDING
TEN EXCHANGE PLACE, SUITE 350
SALT LAKE CITY, UTAH 84111
TELEPHONE: 801.456.7655

RAINA C. BORRELLI*
RAINA@TURKESTRAUSS.COM
TURKE & STRAUSS LLP
613 WILLIAMSON STREET, SUITE 201
MADISON, WI 53703
TELEPHONE: 608.237.1775
*PRO HAC VICE FORTHCOMING

ATTORNEYS FOR PLAINTIFFS AND
PROPOSED CLASS COUNSEL

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

JAMIE KILGORE and B.E., individuals on behalf of themselves and all others similarly situated, Plaintiffs, v. EASTERSEALS-GOODWILL NORTHERN ROCKY MOUNTAIN, INC., a Montana Corporation, Defendant.	**COMPLAINT** **[PROPOSED CLASS ACTION]** **JURY TRIAL DEMANDED** Case No. 2:22-cv-728

Plaintiffs, Jamie Kilgore and B.E. ("Plaintiffs") bring this action on behalf of themselves, and all others similarly situated against Defendant, Easterseals-Goodwill Northern Rocky Mountain, Inc. ("ESGW" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

NATURE OF THE ACTION

1. On or about July 20, 2022, Defendant ESGW, a job skill training non-profit company with Goodwill retail store locations in Idaho, Montana, Utah and Wyoming, discovered that between October 12 and November 11, 2021, certain employee emails were hacked in a data breach by cybercriminals ("Data Breach"). The employee emails contained sensitive and confidential employee and client information including names, Social Security numbers and driver's license numbers ("PII").

2. On information and belief, it is unclear when Defendant first learned of the Data Breach in relation to when Defendant disclosed it and how long the Data Breach carried on undetected.

3. Defendant first disclosed the Data Breach to affected individuals by letter dated September 16, 2022 (the "Breach Notice").

4. When Defendant finally announced the Data Breach, it deliberately underplayed the breach's severity and misrepresented that "we are not aware of any reports of improper use of information as a direct result of this incident" even though Defendant knew cybercriminals had infiltrated its systems. A true and correct copy of the Breach Notice is attached hereto as Exhibit 1.[1]

5. Defendant's failure to timely detect and report the Data Breach made victims vulnerable to identify theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

[1] Breach Notice obtained from Defendant's website, https://www.esgw.org/ (last visited October 26, 2022).

6. Defendant's failure to protect its employees' and consumers' PII and adequately warn them about the Data Breach violates the law, harming current and former ESGW employees, clients and other impacted individuals.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

8. Defendant's misconduct has injured the Plaintiffs and members of the proposed Class in a number of ways, including: (i) the lost or diminished value of their PII; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive PII.

9. Plaintiffs and members of the proposed nationwide Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiffs and members of the proposed Class therefore bring this lawsuit seeking damages and relief for Defendant's actions.

THE PARTIES

11. Plaintiff Jamie Kilgore is an adult resident and citizen of Montana. Ms. Kilgore intends to remain domiciled in Montana indefinitely and maintains her true, fixed and permanent home in Montana. Ms. Kilgore is a former ESGW employee and her PII was compromised by the Data Breach.

12. Plaintiff, B.E. is an adult resident and citizen of Utah. B.E intends to remain domiciled in Utah indefinitely, and maintains his true, fixed, and permanent home in Utah. B.E. is an ESGW employee who works in Utah, and his PII was compromised by the Data Breach.

13. Defendant ESGW is a Montana corporation with its principal place of business located at 425 1st Avenue N, Great Falls, Montana 59401. ESGW is registered to do business in the State of Utah with a registered agent address of 15 West South Temple, Suite 600, Salt Lake City, Utah 84101.

JURISDICTION & VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action in which the amount in controversy exceeds $5 million, exclusive of costs and interest, there are more than 100 members in the proposed class, and at least one class member is a citizen of a different state than ESGW, establishing minimal diversity.

15. This Court has personal jurisdiction over ESGW because it regularly transacts business in Utah.

16. Venue is proper in this Court under 28 U.S.C. §§ 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because ESGW conducts business in this District.

COMMON FACTUAL ALLEGATIONS

Defendant's Failure to Prevent the Data Breach

17. Plaintiff and members of the proposed Class are Defendant's current and former employees, clients and other individuals.

18. To be employed by Defendant, Defendant requires its employees to provide their PII. Similarly, Defendant requires that its client provide PII to Defendant as a condition of providing them services.

19. Defendant maintains records of its employees' and clients' information, including their full names, Social Security Numbers and in some cases, driver's license numbers. These records are stored on Defendant's computer systems.

20. When Defendant collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

21. After the Data Breach occurred, Defendant's CEO Michelle Belknap apologized in an email to employees and stated that Defendant was "continuing to take steps to improve our cybersecurity." A true and correct copy of the email is included as Exhibit 2.

22. Ms. Belknap's email outlines numerous steps and measures Defendant planned to take to improve its cybersecurity following the Data Breach – a concession that Defendant's cybersecurity was deficient prior to the Data Breach. Exh. 2.

23. Defendant represented to its employees, prospective employees and clients that their PII would be secure. Plaintiffs and members of the proposed Class relied on such representations when they agreed to provide their PII to Defendant.

24. Despite its alleged commitments to securing sensitive employee and client data, Defendant does not follow industry standard practices in securing individuals' PII.

25. In October 2021, hackers bypassed Defendants' security safeguards and infiltrated its systems, giving them access to valuable PII.

26. On information and belief, Defendant does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

27. Defendant's negligent conduct caused the Data Breach. Defendant violated its obligation to implement best practices and comply with industry standards concerning computer system security. Defendant failed to comply with security standards and allowed its employees' and clients' PII to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

28. Defendant finally admitted to the Data Breach on or about September 16 2022—months after discovering the Data Breach. Defendant has failed to justify the delays in notifying breach victims.

29. Defendant encouraged Data Breach victims to "take steps to protect themselves against identify theft, including placing a fraud alert/security freeze . . . remaining vigilant in reviewing financial account statements and checking credit reports for fraudulent or irregular activity on a regular basis." Exh. 1.

30. Defendant has instructed breach victims to place a fraud alert on credit files and offered limited identify theft protection services.

31. However, these measures are not sufficient to protect Plaintiffs and the Class from harm. As more fully articulated below, Plaintiffs' and the members of the proposed Class's personal data may exist on the dark web and in the public domain for months, or even years, before it is used for ill gains and actions. With limited credit monitoring, and no form of insurance or other protection, Plaintiffs and members of the proposed Class remain unprotected from the real and long-term threats against their personal, sensitive, and private data.

32. Therefore, the "protection" services offered by Defendant are inadequate, and Plaintiffs and the members of the proposed Class have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

Plaintiff Kilgore's Experience

33. Plaintiff Jamie Kilgore is a former employee of Defendant.

34. As a condition of her employment, Defendant required Plaintiff Kilgore to provide her PII, and Ms. Kilgore provided her PII to Defendant.

35. On or about September 23, 2022, Plaintiff Kilgore received a notice letter from Defendant confirming her PII was compromised as a result of the Data Breach.

36. Since the Data Breach, Ms. Kilgore has experienced fraudulent attempts to use her PayPal account to purchase firearms.

37. Ms. Kilgore has received spam texts and phone calls since the Data Breach.

38. Plaintiff Kilgore has spent, and will have to spend, considerable time and effort over the coming years monitoring her accounts to protect herself from identity theft. Plaintiff Kilgore's personal financial security has been jeopardized and there is uncertainty over what personal information was revealed in the Data Breach.

39. Ms. Kilgore suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant, which was compromised in and as a result of the Data Breach.

40. Ms. Kilgore's privacy has been invaded by the access to and exfiltration of her PII, which is now in the hands of third-parties not authorized to view or possess her PII.

41. Ms. Kilgore has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of criminals. Ms. Kilgore has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy, fraud that he suffered, and risk of future harm.

42. Had Ms. Kilgore known that Defendant does not adequately protect PII, she would not have provided Defendant with her PII. Furthermore, Plaintiff Kilgore's sensitive PII remains in Defendant's possession without adequate protection against known threats, exposing her to the prospect of additional harm in the event Defendant suffers another data breach.

Plaintiff B.E.'s Experience

43. Plaintiff B.E. is a current employee of Defendant.

44. As a condition of his employment, Defendant required Plaintiff B.E. to provide his PII, and B.E. indeed provided his PII to Defendant.

45. In September 2022, Plaintiff B.E. received an email and notice letter from Defendant confirming his PII was compromised as a result of the Data Breach.

46. After receiving news of the Data Breach, Mr. B.E. tried to call Defendant several times to find out more information; when he eventually spoke with one of Defendant's representatives, the person had no additional information.

47. Since the Data Breach, B.E. experienced fraudulent attempts to use his Visa card and Costco membership to purchase products.

48. B.E. has spoken with all three major credit bureaus and frozen his credit. He has paid money to each of the bureaus for fraud protection services and continues to incur monthly expenses to try to protect his identity.

49. B.E. has received phishing emails since the Data Breach.

50. B.E. has spent, and will have to spend, considerable time and effort over the coming years monitoring his accounts to protect himself from identity theft. Plaintiff's personal financial security has been jeopardized and there is uncertainty over what personal information was revealed in the Data Breach.

51. B.E. suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant, which was compromised in and as a result of the Data Breach.

52. B.E.'s privacy has been invaded by the access to and exfiltration of his PII, which is now in the hands of third-parties not authorized to view or possess his PII.

53. B.E. has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals. B.E. has suffered and continues to suffer

annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy, fraud that he suffered, and risk of future harm.

54. Had Plaintiff B.E. known that Defendant does not adequately protect PII, he would not have provided Defendant with his PII. Furthermore, Plaintiff B.E.'s sensitive PII remains in Defendant's possession without adequate protection against known threats, exposing him to the prospect of additional harm in the event Defendant suffers another data breach.

Plaintiffs and the Class Face a Significant Present and Continuing Risk of Identity Theft

55. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

56. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

57. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[2]

58. As a result of Defendant's failure to prevent, and timely report the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses and lost time. They have also suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

[2] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited October 26, 2022).

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying 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 and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

59. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained. [3]

60. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly on various "dark web" internet websites making the information publicly available, for a fee.

[3] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited October 26, 2022).

61. It can take victims years to spot identity PII theft, giving criminals plenty of time to milk that information for cash.

62. One such example of criminals using PII for profit is the development of "Fullz" packages.[4]

63. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

64. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that

[4] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/ (last visited October 26, 2022).

Plaintiffs' and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

65. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, leading to more than $3.5 billion in losses to individuals and business victims.

66. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and the Class that their PII had been stolen.

67. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

68. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

69. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

70. The Federal Trade Commission ("FTC") also has recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner,

Pamela Jones Harbour, stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[5]

71. The FTC has also issued several guidelines for businesses that highlight reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[6] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[7]

72. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve the fallout.[8] The FTC treats 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(a) of the FTC Act.

---

[5] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited October 26, 2022).

[6] *Start With Security, A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited October 26, 2022).

[7] *Id.*

[8] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited October 26, 2022).

73. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

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

75. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system

[9] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[10] *Id.*

logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations.

76. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiffs and potentially thousands of members of the proposed Class to unscrupulous operators, con artists and outright criminals.

77. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

78. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

79. On information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

81. Defendant's failure to properly and promptly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

82. **Definition of the Class.** Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 and DUCivR 23-1(b) on behalf of themselves and all members of the proposed classes (together the "Class"), defined as follows:

> All individuals residing in the United States whose personal information was compromised in the Data Breach disclosed by Defendant in September 2022.

83. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

84. The Class defined above is identifiable through Defendant's business records.

85. Plaintiffs reserve the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

86. Plaintiffs and members of the Class satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23:

a. **Numerosity**. The exact number of the members of the Class is unknown but, upon information and belief, the number of Class members is such that individual joinder in this case is impracticable. Members of the Class can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

b. **Typicality**. Plaintiffs' claims are typical of the claims of other members of the Class in that Plaintiffs, and the members of the Class sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and members of the Class sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

c. **Adequacy**. Plaintiffs will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiffs.

d. **Commonality and Predominance**. There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and members of the Class's PII;

ii. Whether Defendant breached the duty to use reasonable care to safeguard Plaintiffs' and members of the Class's PII;

iii. Whether Defendant breached its contractual promises to safeguard Plaintiffs' and members of the Class's PII;

iv. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

v. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiffs' and members of the Class's PII from unauthorized release and disclosure;

vi. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

vii. Whether Defendant's delay in informing Plaintiffs and members of the Class of the Data Breach was unreasonable;

viii. Whether Defendant's method of informing Plaintiffs and other members of the Class of the Data Breach was unreasonable;

ix. Whether Defendant's conduct was likely to deceive the public;

x. Whether Defendant is liable for negligence or gross negligence;

xi. Whether Plaintiffs and members of the Class were injured as a proximate cause or result of the Data Breach;

xii. Whether Plaintiffs and members of the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiff and members of the Class.

xiii. Whether Defendant's practices and representations related to the Data Breach breached implied warranties.

xiv. What the proper measure of damages is; and

xv. Whether Plaintiffs and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

e. **Superiority:** A class action is also a fair and efficient method of adjudicating the controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured

87. A class action is therefore superior to individual litigation because:

a. The amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

88. Plaintiffs incorporates all previous paragraphs as if fully set forth below.

89. Plaintiffs and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

90. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards for data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who made that happen.

91. In addition, 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.

92. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and

occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

93. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and members of the Class's PII for employment and service purposes. Plaintiffs and members of the Class needed to provide their PII to Defendant to receive training and employment from Defendant, and Defendant retained that information.

94. The risk that unauthorized persons would try to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would try to access Defendant's databases containing the PII—whether by malware or otherwise.

95. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and members of the Class and the importance of exercising reasonable care in handling it.

96. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injuries.

97. Defendant also breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and members of the Class's injuries-in-fact.

98. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiffs, and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

99. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs' and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff and the Class)

100. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

101. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

102. 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 customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the members of the Class's sensitive PII.

103. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

104. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

105. Defendant had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs and the Class's PII.

106. Defendant breached respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

107. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

108. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

109. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

110. Had Plaintiffs and members of the Class known that Defendant would not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

111. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
Breach of Contract, Including the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Class)

112. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

113. Defendant offered employment and services to Plaintiffs and members of the Class.

114. Defendant required Plaintiffs and the members of the Class to provide Defendant with their PII to receive employment and services.

115. In turn, Defendant agreed it would not disclose the PII it collects from employees and clients to unauthorized persons. Defendant also impliedly promised to maintain safeguards to protect its employees' and clients' PII.

116. Class members who are or were employees accepted Defendant's offer of employment by providing their PII to Defendant. Class members who are or were clients accepted Defendant's offer of services by providing their PII to Defendant.

117. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access or theft of their PII.

118. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant without such agreement with Defendant.

119. Defendant materially breached the contracts it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PII;

b. Violating industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

120. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

121. Plaintiffs and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

122. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

123. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

124. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

125. In these and other ways, Defendant violated its duty of good faith and fair dealing.

126. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

127. Plaintiffs, on behalf of themselves and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of the Plaintiffs and the Class)

128. Plaintiffs incorporates all previous paragraphs as if fully set forth below.

129. This claim is plead in the alternative to the Third Claim for Relief.

130. Plaintiffs and members of the Class conferred a benefit upon Defendant in the form employee services and compensation for services received.

131. Defendant appreciated or knew about the benefits conferred upon itself by Plaintiffs and members of the Class. Defendant also benefited from the receipt of Plaintiffs' and members of the Class's PII, as this was used to facilitate employment processing, payroll, and client services.

132. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the proposed Class's services and payments and their PII because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII, nor provided employment services nor paid for Defendant's services had they known Defendant would fail to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and members of the Class paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

133. Defendant should be compelled to disgorge into a common fund to benefit Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

134. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

135. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

136. Defendants owed a duty to its employees and clients including Plaintiffs and the Class, to keep this information confidential.

137. The unauthorized acquisition (*i.e.,* theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

138. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant to receive services and for employment, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

139. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

140. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

141. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

142. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

143. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

144. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

145. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

146. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SIXTH CLAIM FOR RELIEF
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiffs and the Class)

147. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

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

149. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

150. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII with which it is entrusted from its employees and clients, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its employees' and clients' personal information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

151. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its current and former employees' and clients' (*i.e.*, Plaintiffs' and the Class's) data.

152. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

153. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

154. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

DATED this 21st of November, 2022.

MARSHALL OLSON & HULL, PC

BY: /s/ Trevor C. Lang
JASON R. HULL
TREVOR C. LANG

TURKE & STRAUSS, LLP
RAINA C. BORRELLI

ATTORNEYS FOR PLAINTIFFS AND
PROPOSED CLASS COUNSEL

ClassAction.org