Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Michelle Puller-Soto, on behalf of herself and all others similarly situated, Plaintiff, v. **UNITE HERE,** Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Michelle Puller-Soto ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against UNITE HERE ("Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against UNITE HERE for its failure to properly secure and safeguard Plaintiff's and other similarly situated UNITE HERE union members' personally identifiable information ("PII") and protected health information ("PHI"), including names, Social Security numbers, dates of birth, and medical information (the "Private Information"), from criminal hackers.

2. UNITE HERE, based in New York, New York, is a labor union that serves hundreds of thousands of workers throughout the United States and Canada.

3. On or about February 23, 2024, UNITE HERE filed official notice of a hacking incident with the Maine Office of the Attorney General.[1] Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or around the same time, UNITE HERE also sent out data breach letters (the "Notice") to individuals whose Private Information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiff and "Class Members" (defined below), unusual activity was detected on some of its computer systems on October 20, 2023. In response, Defendant launched an investigation which revealed that an unauthorized party had access to certain files that contained sensitive union member information, with such access taking place during an undisclosed period of time (the "Data Breach"). Four months passed from the time UNITE HERE became aware of the Breach to the time it notified impacted union members that they were at risk.

6. As a result of this delayed response, Plaintiff and Class Members had no idea for *four months* that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive union member data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers and medical information that UNITE HERE collected and maintained.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/5aeae259-5615-4ba6-9108-ea36011727ee.shtml (last visited Feb. 29, 2024).

Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by UNITE HERE that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address UNITE HERE's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to UNITE HERE, and thus UNITE HERE was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, UNITE HERE failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had UNITE HERE properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of UNITE HERE's negligent conduct as the Private Information that UNITE HERE collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for Negligence, Negligence *Per Se*, Breach of Contract, Breach of Implied Contract, Unjust Enrichment, Breach of Fiduciary Duty, Breach of Confidence, Breach of Third-Party Beneficiary Contract, and Declaratory Judgment.

II. PARTIES

17. Plaintiff Michelle Puller-Soto is, and at all times mentioned herein was, an individual citizen of the State of Washington.

18. Defendant UNITE HERE is a labor union with its principal place of business at 275 7th Avenue, 16th Floor, New York, New York, 10001.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many

of whom have different citizenship from UNITE HERE. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over UNITE HERE because UNITE HERE operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and UNITE HERE has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. UNITE HERE's Business and Collection of Plaintiff's and Class Members' Private Information

22. UNITE HERE is a labor union that represents hundreds of thousands of workers in the hospitality industry across the United States. Founded in 2004, UNITE HERE was formed by the merger of UNITE (the Union of Needletrades, Industrial, and Textiles Employees) and HERE (the International Union of Hotel Employees and Restaurant Employees). UNITE HERE employs more than 379 people and generates approximately $91.9 million in annual revenue.

23. As a condition of receiving union representation, UNITE HERE requires that its union members entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from UNITE HERE, Plaintiff and Class Members were required to provide their Private Information to Defendant.

24. In the Notice Letter, UNITE HERE stated that "the confidentiality, privacy, and security of information in our care is one of our highest priorities."[2] Also, in its Notice of Privacy Policy, UNITE HERE informs its union members that it "makes every effort to ensure the secure

[2] *See* Notice Letter.

collection and transmission of your sensitive information using industry accepted data collection and encryption methodologies, such as SSL (Secure Sockets Layer)."[3]

25. Thus, due to the highly sensitive and personal nature of the information UNITE HERE acquires and stores with respect to its union members, UNITE HERE, upon information and belief, promises to, among other things: keep union members' Private Information private; comply with industry standards related to data security and the maintenance of its union members' Private Information; inform its union members of its legal duties relating to data security and comply with all federal and state laws protecting union members' Private Information; only use and release union members' Private Information for reasons that relate to the services it provides; and provide adequate notice to union members if their Private Information is disclosed without authorization.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, UNITE HERE assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

27. Plaintiff and Class Members relied on UNITE HERE to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members

28. According to Defendant's Notice, it learned of unauthorized access to its computer systems on an undisclosed date, with such unauthorized access having taken place on October 20, 2023.

[3] *See* https://unitehere.org/privacy-policy/ (last visited Feb. 29, 2024).

29. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including members' names, Social Security numbers, date of birth, and medical information.

30. On or about February 23, 2023, roughly four months after UNITE HERE learned that the Class's Private Information was first accessed by cybercriminals, UNITE HERE finally began to notify union members that its investigation determined that their Private Information was affected.

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

32. Plaintiff and Class Members provided their Private Information to UNITE HERE with the reasonable expectation and mutual understanding that UNITE HERE would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

33. UNITE HERE's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

34. UNITE HERE knew or should have known that its electronic records would be targeted by cybercriminals.

35. UNITE HERE was on notice that companies dealing with sensitive PII and PHI are susceptible targets for data breaches.

36. UNITE HERE was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health

Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[4]

37. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their union members' confidential information:

> Cybersecurity is not just a technical issue; it's a union member safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of union members' health and financial information, but also union member access to care.[5]

38. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[6]

39. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty

[4] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on Feb. 29, 2024).

[5] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on Feb. 29, 2024).

[6] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on Feb. 29, 2024).

percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[7]

40. As a labor union that collects both PII and PHI, UNITE HERE knew, or should have known, the importance of safeguarding its union members' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on UNITE HERE's members as a result of a breach. UNITE HERE failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

C. UNITE HERE Failed to Comply with HIPAA

41. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

42. UNITE HERE's Data Breach resulted from a combination of insufficiencies that indicate its failure to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from UNITE HERE's Data Breach that UNITE HERE either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

43. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

[7] *Id.*

44. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

45. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

46. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

47. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

48. Based upon Defendant's Notice to Plaintiff and Class Members, UNITE HERE reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

49. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

50. UNITE HERE reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

51. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach,

and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

52. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

53. UNITE HERE reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

54. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

55. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

56. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

57. In addition, UNITE HERE's Data Breach could have been prevented if UNITE HERE had implemented HIPAA mandated, industry standard policies and procedures for securely

disposing of PHI when it was no longer necessary and/or had honored its obligations to its union members.

58. UNITE HERE's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information UNITE HERE creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy

rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

59. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required UNITE HERE to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

60. Because UNITE HERE has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure UNITE HERE's approach to information security is adequate and appropriate going forward. UNITE HERE still maintains the PHI and other highly sensitive PII of its current and former union members, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

D. UNITE HERE Failed to Comply with FTC Guidelines

61. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and

appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

62. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into 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.

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

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

65. As evidenced by the Data Breach, UNITE HERE failed to properly implement basic data security practices. UNITE HERE's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

66. UNITE HERE was at all times fully aware of its obligation to protect the Private Information of its union members yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. UNITE HERE Failed to Comply with Industry Standards

67. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

68. Some industry best practices that should be implemented by businesses dealing with sensitive PII and PHI like UNITE HERE include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow at least some or all of these industry best practices.

69. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

70. 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.

71. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. UNITE HERE Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

72. As demonstrated by the obligations set forth in both HIPAA and the FTCA, UNITE HERE owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. UNITE HERE owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

73. UNITE HERE breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. UNITE HERE's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect union members' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its union members Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

74. UNITE HERE negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

75. Had UNITE HERE remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

76. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with UNITE HERE.

G. UNITE HERE Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

77. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such

as data breaches or unauthorized disclosure of data.[8] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

78. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

79. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

80. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

[8] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Feb. 29, 2024).

Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

81. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

82. One such example of this is the development of "Fullz" packages.

83. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

84. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen 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 Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

85. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[9] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

86. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

87. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[10]

88. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

---

[9] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Feb. 29, 2024).

[10] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Feb. 29, 2024).

89. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[11]

90. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

91. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[12]

92. The ramifications of UNITE HERE's failure to keep its members' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

93. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities

[11] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Feb. 29, 2024).

[12] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Feb. 29, 2024).

notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

94. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[13]

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

95. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

96. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiff's and Class Members' Damages

Plaintiff Michelle Puller-Soto's Experience

97. Plaintiff Puller-Soto became a union member of UNITE HERE in or around 2020.

98. When Plaintiff Puller-Soto became a union member, Defendant required Plaintiff Puller-Soto provide it with substantial amounts of her Private Information, including PHI.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Feb. 29, 2024).

99. On or about February 23, 2024, Plaintiff Puller-Soto received the Notice informing her that her Private Information had been affected during the Data Breach. The notice letter informed her that the Private Information stolen included her "name, Social Security number, date of birth, medical information."

100. The notice letter offered Plaintiff Puller-Soto only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Puller-Soto will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

101. Plaintiff Puller-Soto suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

102. Plaintiff Puller-Soto would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its union members' personal and health information from theft, and that those systems were subject to a data breach.

103. Plaintiff Puller-Soto suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

104. Plaintiff Puller-Soto suffered actual injury in the form of damages to and diminution in the value of her personal and health information – a form of intangible property that Plaintiff Puller-Soto entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

105. Plaintiff Puller-Soto suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

106. Plaintiff Puller-Soto has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

107. As a result of the Data Breach, Plaintiff Puller-Soto made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Puller-Soto has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

108. As a result of the Data Breach, Plaintiff Puller-Soto has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Puller-Soto is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

109. Plaintiff Puller-Soto also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendant obtained from Plaintiff Puller-Soto; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

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

111. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

112. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

113. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

114. As a direct and proximate result of UNITE HERE's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns and insurance claims filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

115. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

116. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

117. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

118. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

119. Plaintiff and Class Members also lost the benefit of the bargain they made with UNITE HERE. Plaintiff and Class Members entrusted their inherently valuable Private Information to UNITE HERE in exchange for adequate data security that was never actually implemented. Thus, Plaintiff and the Class did not receive the benefit of the bargain.

120. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth

roughly $200 billion.[14] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[15]

121. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

122. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

123. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of UNITE HERE, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its union members is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

---

[14] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Feb. 29, 2024).

[15] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Feb. 29, 2024).

124. As a direct and proximate result of UNITE HERE's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

125. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

126. Specifically, Plaintiff proposes the following Nationwide Class definition (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/ or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

127. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

128. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well as add subclasses before the Court determines whether certification is appropriate.

129. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

130. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 791,273 current and former union members of UNITE HERE whose data was compromised in the Data Breach. The identities of Class

Members are ascertainable through UNITE HERE's records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether UNITE HERE engaged in the conduct alleged herein;

b. Whether UNITE HERE's conduct violated the FTCA and HIPAA;

c. When UNITE HERE learned of the Data Breach;

d. Whether UNITE HERE's response to the Data Breach was adequate;

e. Whether UNITE HERE unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether UNITE HERE failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

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

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

i. Whether UNITE HERE owed a duty to Class Members to safeguard their Private Information;

j. Whether UNITE HERE breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether UNITE HERE had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether UNITE HERE breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether UNITE HERE knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of UNITE HERE's misconduct;

p. Whether UNITE HERE's conduct was negligent;

q. Whether UNITE HERE's conduct was *per se* negligent;

r. Whether UNITE HERE was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

132. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of UNITE HERE. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members,

and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

133. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

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

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

136. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). UNITE HERE has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

137. Finally, all members of the proposed Class are readily ascertainable. UNITE HERE has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by UNITE HERE.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

138. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

139. UNITE HERE knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

140. UNITE HERE's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

141. UNITE HERE knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. UNITE HERE was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

142. UNITE HERE owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. UNITE HERE's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect union members' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

143. UNITE HERE's duty to employ reasonable data security measures arose, in part, 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.

144. UNITE HERE's duty also arose because Defendant was bound by industry standards to protect its union members' confidential Private Information.

145. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, which owed them a duty of care to not subject them to an unreasonable risk of harm.

146. UNITE HERE, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within UNITE HERE's possession.

147. UNITE HERE, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

148. UNITE HERE, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

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

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

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

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

150. UNITE HERE acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

151. UNITE HERE had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust UNITE HERE with their Private Information was predicated on the understanding that UNITE HERE would take adequate security precautions. Moreover, only UNITE HERE had the ability to protect its systems (and the Private Information that it stored on them) from attack.

152. UNITE HERE's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

153. As a result of UNITE HERE's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

154. UNITE HERE's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

155. As a result of UNITE HERE's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

156. UNITE HERE also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

157. As a direct and proximate result of UNITE HERE's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

158. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

159. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

160. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring UNITE HERE to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

161. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

162. Pursuant to Section 5 of the FTCA, UNITE HERE had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

163. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., UNITE HERE had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

164. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

165. UNITE HERE breached its duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

166. Specifically, UNITE HERE breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

167. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of UNITE HERE's duty in this regard.

168. UNITE HERE also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

169. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to UNITE HERE's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

170. Plaintiff and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and UNITE HERE's failure to comply with both constitutes negligence *per se*.

171. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to UNITE HERE's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

172. As a direct and proximate result of UNITE HERE's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

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

174. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring UNITE HERE to, *inter alia*, strengthen its data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

175. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

176. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of being union members.

177. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

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

179. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f)

retain the Private Information only under conditions that kept such information secure and confidential.

180. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

181. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

182. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

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

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

185. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

186. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

187. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

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

189. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

190. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

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

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

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

193. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

194. Defendant entered into contracts, written or implied, with its clients (local labor unions and health funds) to perform services that include, but are not limited to, providing union representation to its clients' members – including Plaintiff and Class Members. Upon information and belief, these contracts are virtually identical between and among Defendant and its clients around the country whose members, including Plaintiff and Class Members, were affected by the Data Breach.

195. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information belonging to Plaintiff and the Class.

196. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, then Plaintiff and Class Members would be harmed.

197. Defendant breached these contracts by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

198. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

199. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

200. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

201. This Count is pleaded in the alternative to Counts III and IV above.

202. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the union representation that was the subject of the transaction and should have had their Private Information protected with adequate data security.

203. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

204. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

205. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

206. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendant or become union members at Defendant.

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

208. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

209. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Keown's Private Information being disseminated on the dark web, according to Discover; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

210. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

211. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

212. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

213. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by UNITE HERE and ultimately accessed and acquired in the Data Breach.

214. As a labor union, UNITE HERE has a special, fiduciary relationship with its union members, including Plaintiff and Class Members. Because of that special relationship, UNITE HERE was provided with and stored Plaintiff's and Class Members' Private Information and had a duty to maintain such Information in confidence.

215. Union members like Plaintiff and Class Members have a privacy interest in personal medical and other matters, and UNITE HERE had a duty not to disclose such matters concerning its union members.

216. As a result of the parties' relationship, UNITE HERE had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiff and Class Members, information that was not generally known.

217. Plaintiff and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

218. UNITE HERE breached its duty of confidence owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of union member information that resulted in the unauthorized access and compromise of Plaintiff's and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its union members; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class members' Private Information to a criminal third party.

219. But for UNITE HERE's wrongful breach of its duty of confidence owed to Plaintiff and Class Members, their Private Information would not have been compromised.

220. As a direct and proximate result of UNITE HERE's wrongful breach of its duty of confidence, Plaintiff and Class Members have suffered and will continue to suffer the injuries alleged herein.

221. It would be inequitable for UNITE HERE to retain the benefit of controlling and maintaining Plaintiff's and Class Members' Private Information at the expense of Plaintiff and Class Members.

222. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

223. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

224. 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 that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

225. UNITE HERE owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

226. UNITE HERE still possesses Private Information regarding Plaintiff and Class Members.

227. Plaintiff alleges that UNITE HERE's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromises of her Private Information will occur in the future.

228. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. UNITE HERE owes a legal duty to secure its members' Private Information and to timely notify its members of a data breach under the common law, HIPAA, and the FTCA;

b. UNITE HERE's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect union members' Private Information; and

c. UNITE HERE continues to breach this legal duty by failing to employ reasonable measures to secure union members' Private Information.

229. This Court should also issue corresponding prospective injunctive relief requiring UNITE HERE to employ adequate security protocols consistent with legal and industry standards to protect union members' Private Information, including the following:

a. Order UNITE HERE to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, UNITE HERE must implement and maintain reasonable security measures, including, but not limited to:

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

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of UNITE HERE's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its union members about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

230. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at UNITE HERE. The risk of another such breach is real, immediate, and substantial. If another breach at UNITE HERE occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

231. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to UNITE HERE if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of UNITE HERE's compliance with an injunction requiring reasonable prospective data security

measures is relatively minimal, and UNITE HERE has a pre-existing legal obligation to employ such measures.

232. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at UNITE HERE, thus preventing future injury to Plaintiff and other union members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class and requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing UNITE HERE to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring UNITE HERE to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: February 29, 2024

Respectfully submitted,

/s/ Mason A. Barney

Mason A. Barney (SDNY Bar No. MB7225)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com