Exhibit A1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re UNITE HERE DATA SECURITY INCIDENT LITIGATION	Lead Case No. 1:24-cv-01565 (Consolidated with Case No. 1:24-cv-01904)
This Document Relates To: ALL ACTIONS.	CLASS ACTION JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

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

I. INTRODUCTION

1. Plaintiffs bring this class action against UNITE HERE for its failure to properly secure and safeguard Plaintiffs' and other similarly situated UNITE HERE union members' personally identifiable information ("PII") and protected health information ("PHI"), including their 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 an 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 that Defendant sent to Plaintiffs 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 that 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, Plaintiffs 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. This risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive and confidential personal 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.

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

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 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. Therefore, Plaintiffs 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.

10. Plaintiffs bring 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 Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

11. The potential for improper disclosure and theft of Plaintiffs' 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.

12. 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.

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

14. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and continuing risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

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

16. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

17. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

18. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct.

II. PARTIES

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

20. Plaintiff Tamiko Conway is, and at all times mentioned herein was, an individual citizen of the State of Michigan.

21. 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

22. 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).

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

24. 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 Plaintiffs' and Class Members' Private Information

25. 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.

26. As a condition of receiving union representation and other benefits, 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, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

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

28. 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 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.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, UNITE HERE assumed legal and equitable duties it owed to them

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

and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

30. 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 Plaintiffs and Class Members

31. 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.

32. 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.

33. 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.

34. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of

this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

36. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its union members' Private Information safe and confidential.

37. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

38. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

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

41. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[4]

42. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

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

records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

43. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[5]

44. Additionally, as companies became more dependent on computer systems to run their business,[6] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[7]

45. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

---

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

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

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

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

48. 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. **Data Breaches are Preventable.**

49. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

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

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

should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[8]

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

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[9]

52. Given that Defendant was storing the Private Information of its union members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

53. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of over seven hundred thousand individuals, including Plaintiffs and Class Members.

D. UNITE HERE Failed to Comply with FTC Guidelines

54. 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

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

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).

55. 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.

56. 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.

57. 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.

58. 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 Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

59. 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

60. 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.

61. 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.

62. 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.

63. 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.

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

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

65. As demonstrated by the obligations set forth in the FTCA, UNITE HERE owed a duty to Plaintiffs 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 Plaintiffs 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

66. UNITE HERE breached its obligations to Plaintiffs 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; and

f. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

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

68. 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 Plaintiffs' and Class Members' confidential Private Information.

69. Accordingly, Plaintiffs' 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. Plaintiffs 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

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

as data breaches or unauthorized disclosure of data.[10] 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.

71. 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.

72. 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.

73. 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."

[10] *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.

74. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' 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 Plaintiffs and Class Members.

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

76. 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.

77. 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 Plaintiffs' 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 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 Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

78. 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.[11] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

79. 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.

80. 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.[12]

81. 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.

---

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

[12] 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).

82. 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.[13]

83. 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.

84. 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."[14]

85. 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.

86. 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

[13] 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).

[14] 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.

87. 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:[15]

> [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.

88. 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.

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

H. Plaintiffs' and Class Members' Damages

Plaintiff Michelle Puller-Soto's Experience

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

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

[15] *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).

92. 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, [and] medical information."

93. 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.

94. 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.

95. 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.

96. 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.

97. 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.

98. 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.

99. 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.

100. 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.

101. 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.

102. 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.

103. 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.

Plaintiff Tamiko Conway's Experience

104. Plaintiff Tamiko Conway is a current union member at UNITE.

105. As a condition of her union membership at UNITE, Plaintiff Conway was required to provide her Private Information to Defendant, including her name, Social Security number, and other sensitive information.

106. At the time of the Data Breach—on or about October 20, 2023—Defendant retained Plaintiff Conway's Private Information in its system.

107. Plaintiff Conway is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Conway would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

108. Plaintiff Tamiko Conway received the Notice Letter, by U.S. mail, directly from Defendant, dated February 23, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name and Social Security number.

109. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Conway to, among other things, "[r]eview your account statements and credit reports for suspicious activity or errors[,]"[16] Plaintiff Conway made reasonable efforts to

[16] Notice Letter

mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, disputing fraudulent charges on her accounts, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Conway has spent significant time dealing with the Data Breach—valuable time Plaintiff Conway otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

110. Plaintiff Conway suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her 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) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her 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.

111. Plaintiff Conway further suffered actual injury in the form of experiencing fraudulent charges, for approximately $242, to her Chime checking account, in or about October 2023, which, upon information and belief, was caused by the Data Breach.

112. Plaintiff Conway also suffered actual injury in the form of experiencing fraudulent charges, for approximately $100, to her Chime credit card, in or about February 2024, which, upon information and belief, was caused by the Data Breach.

113. Plaintiff Conway additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

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

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

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

117. Plaintiff Tamiko Conway has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

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

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

120. 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.

121. As a direct and proximate result of UNITE HERE's actions and omissions, Plaintiffs 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.

122. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs 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.

123. Plaintiffs 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.

124. Plaintiffs 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 Plaintiffs and Class Members.

125. 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 Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

126. Thus, due to the actual and imminent risk of identity theft, Defendant's Notice Letter encourages Plaintiffs and Class Members to be vigilant against identity theft and fraud and to "[r]eview your account statements and credit reports for suspicious activity or errors."

127. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, disputing fraudulent charges placed on their accounts, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

128. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

129. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

130. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches

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

("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[19]

131. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to be a union member at Defendant, Plaintiffs and other reasonable union members understood and expected that their membership dues were, in part, intended to fund adequate data security practices to protect their Private Information, when in fact, Defendant did not provide the expected data security and instead diverted those funds to its own profit. Accordingly, Plaintiffs and Class Members received union services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

132. Additionally, Plaintiffs 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.[20] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[21]

133. As a result of the Data Breach, Plaintiffs' 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

[19] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[20] *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).

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

happened with no consideration paid to Plaintiffs 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 Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

134. Finally, Plaintiffs 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.

135. Moreover, Plaintiffs 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.

136. As a direct and proximate result of UNITE HERE's actions and inactions, Plaintiffs 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

137. Plaintiffs bring 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).

138. Specifically, Plaintiffs propose 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.

139. 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.

140. Plaintiffs reserve 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.

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

142. 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.

143. 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 other statutes;

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 Plaintiffs' 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 Plaintiffs and the Class Members;

m. Whether UNITE HERE breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

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

144. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' 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. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

146. Predominance. UNITE HERE has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' 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.

147. 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.

148. 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.

149. 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 PLAINTIFFS AND THE NATIONWIDE CLASS)

150. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

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

152. 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.

153. UNITE HERE knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs 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.

154. UNITE HERE owed a duty of care to Plaintiffs 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 Plaintiffs and Class Members;

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

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

155. 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.

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

157. Plaintiffs 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.

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

159. 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 Plaintiffs and Class Members.

160. 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.

161. 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.

162. UNITE HERE acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that

Plaintiffs 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.

163. UNITE HERE had a special relationship with Plaintiffs and Class Members. Plaintiffs' 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.

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

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

166. UNITE HERE's breaches of duty also caused a substantial, imminent risk to Plaintiffs 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.

167. As a result of UNITE HERE's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs 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.

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

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

170. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

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

172. In addition to monetary relief, Plaintiffs 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 Plaintiffs and Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

173. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

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

175. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs 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 Plaintiffs and the Class if their data had been breached and compromised or stolen.

176. In entering into such implied contracts, Plaintiffs 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.

177. Implicit in the agreement between Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

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

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

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

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

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

183. Plaintiffs 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.

184. Plaintiffs 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.

185. Plaintiffs 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.

186. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

187. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs 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.

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

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

190. Plaintiffs 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 III
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

191. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

192. This Count is pleaded in the alternative to Count II above.

193. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information and payment of membership dues. In exchange, Plaintiffs 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.

194. Defendant knew that Plaintiffs 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 and payments made to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

195. When paying membership dues to Defendant, Plaintiffs and Class Members understood that a portion of their payments would be allocated to data security sufficient to protect their PII. Rather than fund such security, Defendant instead diverted that money to its own profit and realized a monetary benefit as a result.

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

197. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate data security practices previously alleged.

198. If Plaintiffs 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.

199. Plaintiffs and Class Members have no adequate remedy at law.

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

201. As a direct and proximate result of Defendant's conduct, Plaintiffs 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) Plaintiffs 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.

202. Plaintiffs 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 Plaintiffs and Class Members may seek restitution or compensation.

203. Plaintiffs 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 IV
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

204. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

205. Plaintiffs 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.

206. As a labor union, UNITE HERE has a special, fiduciary relationship with its union members, including Plaintiffs and Class Members. Because of that special relationship, UNITE

HERE was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to maintain such Information in confidence.

207. Union members like Plaintiffs 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. UNITE HERE was in an exclusive position to protect against the disclosure of Plaintiffs' and Class Members' Private Information.

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

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

210. UNITE HERE breached its duty of confidence owed to Plaintiffs 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 Plaintiffs' 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 Plaintiffs' and Class members' Private Information to a criminal third party.

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

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

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

214. Plaintiffs 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 V
VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT ("GBL")
NEW YORK GEN. BUS. LAW § 349
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

215. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

216. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiffs and the Class by representing that it would maintain adequate data privacy and security practices and procedures to

safeguard Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiffs and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' Private Information;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

217. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

218. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

219. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendant's network and aggregation of Private Information.

220. The representations upon which current and former union members (including Plaintiffs and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and current and former union members (including Plaintiffs and Class Members) relied on those representations to their detriment.

221. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

222. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' Private Information and that the risk of a data security incident was high.

223. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing labor union representation services to consumers in the State of New York.

224. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages.

225. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiffs and the Class Members suffered damages 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) statutory damages; (ix) nominal damages; and (x) 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.

226. As a result, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

227. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members, and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

228. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

229. Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

230. Also, as a direct result of Defendant's violation of GBL § 349, Plaintiffs and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to,

ordering Defendant to: (i) strengthen their 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 VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

231. 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.

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

233. UNITE HERE still possesses Private Information regarding Plaintiffs and Class Members.

234. Plaintiffs allege that UNITE HERE's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of Private Information will occur in the future.

235. 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 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.

236. 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 Plaintiffs 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.

237. If an injunction is not issued, Plaintiffs 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, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

238. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to UNITE HERE if an injunction is issued. Plaintiffs 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.

239. 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 Plaintiffs and other union members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek 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 Plaintiffs are proper representatives of the Nationwide Class and requested herein;

b. Judgment in favor of Plaintiffs 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 Plaintiffs 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 Plaintiffs 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

Plaintiffs demand a trial by jury on all triable issues.

DATED: April 12, 2024.

Respectfully submitted,

/s/ Mason A. Barney
Mason A. Barney (S.D.N.Y. 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

Vicki J. Maniatis (2578896)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Tel: (865) 412-2700
E: vmaniatis@milberg.com

John J. Nelson (CA SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Tel: (858) 209-6941
E: jnelson@milberg.com

Counsel for Plaintiffs and the Proposed Class