THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PAUL CULBERTSON, WILLIAM GIBSON, TIMOTHY SYLVESTER, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, v. DELOITTE CONSULTING LLP Defendant.	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Paul Culbertson, William Gibson, and Timothy Sylvester, individually and on behalf of a class of persons similarly situated (the "Class" or "Class Members"), brings this class action against Defendant Deloitte Consulting LLP ("Deloitte" or "Defendant") seeking equitable relief and damages as set forth below. All allegations made in this Complaint are based upon information and belief except those allegations that pertain to Plaintiffs, which are based on personal knowledge. Each allegation in this Complaint either has evidentiary support or, alternatively, pursuant to Rule 11(b)(3) of the Federal Rules of Civil Procedure, is likely to have evidentiary support after a reasonable opportunity for further investigation or discovery.

PRELIMINARY STATEMENT

1. Plaintiffs bring this action against Defendant for its failure to secure and safeguard their personally identifiable information ("PII").

2. Defendant Deloitte Consulting contracts with various state agencies—including the Ohio Department of Job and Family Services ("ODJFS"), the Illinois Department of Employment Security ("IDES"), and the Colorado Department of Labor and Employment ("CDLE")—to assist

states to administer the federal Pandemic Unemployment Assistance program by creating and maintaining web-based portals through which applicants may apply for benefits and communicate with the state agencies.

3. In May 2020, officials from ODJFS, IDES, and CDL publicly confirmed that their computerized unemployment systems designed, built and maintained by Deloitte allowed public access to applicants' PII, including Social Security numbers, thereby exposing sensitive private data of an unknown number of people who had recently filed for unemployment benefits to unauthorized persons. Upon information and belief, Plaintiffs believe the number of unemployment applicants whose PII was exposed numbers in the hundreds of thousands.

4. Plaintiffs Paul Culbertson, William Gibson, and Timothy Sylvester each applied for unemployment benefits through the ODJFS' web-based portal.

5. On May 20, 2020, Plaintiffs each received correspondence from ODJFS notifying them of the breach and recommending that they "may want to monitor [their] credit," place a "fraud alert" on their credit files, and place a "security freeze" on their credit reports.

6. Plaintiffs bring this action on behalf of themselves and other similarly situated applicants who had their PII exposed as a result of Defendant's failure to protect applicants' PII.

JURISDICTION AND VENUE

7. The jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) (Class Action Fairness Act) in that this is a putative class action with more than 100 class members, more than $5 million in controversy, and the requisite diversity of citizenship.

8. Venue is appropriate pursuant to 28 U.S.C. § 1391. A substantial portion of the events and conduct giving rise to the violations alleged in this Complaint occurred in this District.

9. This Court has personal jurisdiction over Defendant because it has continuous and systematic contacts with this forum, maintains its corporate headquarters in this District, and the events giving rise to this matter arose out of those contacts.

PARTIES

10. Plaintiff Paul Culbertson is a citizen and resident of Akron, Ohio.

11. Plaintiff William Gibson is a citizen and resident of Sandusky, Ohio.

12. Plaintiff Timothy Sylvester is a citizen and resident of Cincinnati, Ohio.

13. Defendant Deloitte Consulting LLP is a limited liability partnership organized under the laws of Delaware and registered to operate in New York State. Its headquarters and principal place of business is located in this District at 30 Rockefeller Plaza, New York, NY 10112.

STATEMENT OF COMMON FACTS

14. Pandemic Unemployment Assistance ("PUA") is a federal program that expands unemployment insurance eligibility to self-employed workers, freelancers, independent contractors, and part-time workers impacted by the coronavirus pandemic in 2020. PUA is one of the programs established by the Coronavirus Aid, Relief, and Economic Security ('CARES") Act, a $2 trillion coronavirus emergency stimulus package that President Trump signed into law on March 27, 2020. The Act expands states' ability to provide unemployment insurance to many workers affected by COVID-19, including people who would not otherwise be eligible for unemployment benefits.

15. Deloitte provides public sector labor and employment services to states, including unemployment insurance solutions. These include claims services, benefit payments control, reporting services, administrative services, and document management services.[1]

[1] https://www2.deloitte.com/us/en/pages/public-sector/solutions/unemployment-insurance-services.html

16. Because Defendant is entrusted with applicants' PII, it has a duty to applicants to keep their PII secure.

17. Defendant knew that safeguarding applicants' PII is vitally important, and regularly represents itself to have robust security features to protect PII.

18. Applicants, such as Plaintiffs and the Class, reasonably expect that when they provide PII to a company, the company will safeguard their PII.

19. Operating in the space that it operates within, Defendant is also well aware of the numerous data breaches that have occurred throughout the United States as well as its responsibility for safeguarding users' PII.

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

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

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

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

21. The U.S. Federal Trade Commission ("F.T.C.") publishes guides for businesses for cybersecurity[2] and protection of PII[3] which includes basic security standards applicable to all types of business.

22. The F.T.C. recommends that businesses:

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

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

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

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

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

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

[2] Start with Security: A Guide for Business, F.T.C. (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[3] Protecting Personal Information: A Guide for Business, F.T.C. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

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

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

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

23. Because the PUA program required a new processing system to handle the different types of claims which are distinct from regular employment, states—including Ohio, Illinois, and Colorado—contracted with Deloitte to design a cloud-based portal system.

24. The PUA program went "live" on or about May 11, 2020.

25. On May 15, 2020, Illinois State Representative Terri Bryant sent a letter to Illinois Governor Pritzker notifying him that a constituent "stumbled upon" a spreadsheet on the IDES

portal containing PII of "thousands of unemployment applicants"—including name, address, social security number, and unemployment claimant ID number.[4]

26. On May 17, 2020, officials from IDES confirmed that IDES was aware of a software "glitch" in the new PUA system designed and maintained by Deloitte that made "some private information publicly available for a short time and worked to immediately remedy the situation."[5]

27. On May 18, 2020, officials from CDLE confirmed that it too experienced a "data access issue" with the new PUA system, which allowed strangers to view applicants' PII.[6] The CDLE assured, however, that "[o]ur vendor partner Deloitte worked swiftly once the unauthorized access was identified and fixed the issue within one hour."[7]

28. On May 20, 2020, ODJFS notified PUA program claimants by email that a security vulnerability in the PUA system designed and maintained by Deloitte allowed third party access to their names, social security number, and home address.

29. Plaintiffs became aware of the breach when they received emails from ODJFS.

30. Since learning of the breach, Plaintiffs Culbertson, Gibson, and Sylvester have been forced to take multiple precautionary steps to protect themselves and their property in an effort to avoid becoming a victim of identity fraud. To this end, Plaintiffs Culbertson, Gibson, and Sylvester have expended time and effort they would have otherwise taken to themselves to: scan their credit card and bank statements; file reports with the Federal Trade Commission; and take extra precautions to carefully review their emails to avoid opening unrecognized emails. In

[4] https://repbryant.com/2020/05/16/rep-bryant-demands-governor-answer-questions-involving-potential-massive-ides-unemployment-applicant-data-breach/
[5] https://patch.com/illinois/across-il/illinois-unemployment-website-glitch-leaks-personal-information
[6] https://www.kktv.com/content/news/Colorado-Labor-Department-confirms-brief-data-exposure-for-pandemic-unemployment-claimants-570633261.html
[7] https://www.kktv.com/content/news/Colorado-Labor-Department-confirms-brief-data-exposure-for-pandemic-unemployment-claimants-570633261.html

addition, Plaintiff Gibson has begun the process of changing his passwords across myriad accounts, requiring additional time and effort he would have otherwise spent at his own leisure.

31. Plaintiffs allege upon information and belief that Defendant's substandard security practices were a direct and proximate cause for the massive data breach compromising the PII of hundreds of thousands of Americans.

32. Plaintiffs allege upon information and belief that Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

33. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiffs' PII, Plaintiffs and Class Members have been damaged.

34. Plaintiffs and Class Members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and will likely incur additional damages in order to prevent and mitigate credit fraud or identity theft. The information exposed in the data breach is, by its very nature, the information necessary to obtain unemployment benefits, apply for and obtain lines of credit, and myriad financially-related activities.

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

cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

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

CLASS ALLEGATIONS

37. Plaintiffs bring this Complaint on behalf of themselves and the following Class ("Nationwide Class"):

> All persons whose personal information was compromised as a result of the PUA portal data breach.

38. The Class and definition specifically excludes: (a) any persons or other entity currently related to or affiliated with Defendant; (b) any Judge presiding over this action and members of his or her family; and (c) all persons who properly execute and file a timely request for exclusion from the Class.

39. Class-wide adjudication of Plaintiffs' claims is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

40. *Numerosity*: The Class Members are so numerous that joinder of individual claims is impracticable. Since the COVID-19 pandemic, approximately 38.6 million U.S. residents have filed for unemployment. Although the precise number is not yet known to Plaintiffs, Plaintiffs reasonably approximate that the number of class members is in the hundreds of thousands.[8] The Class Members can be readily identified through Defendant's records.

[8] *See, e.g.*, https://www.nbcnews.com/business/economy/unemployment-claims-state-see-how-covid-19-has-destroyed-job-n1183686 (total unemployment claims since March 14, 2020: 407,861 in Colorado; 1,039,231 in Illinois; and 1,219,870 in Ohio (last accessed May 21, 2020).

41. *Commonality*: There are significant questions of fact and law common to the Class Members. These issues include but are not limited to:

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

b. Whether Defendant breached that duty or those duties;

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

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

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

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

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

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

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

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

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

42. *Typicality*: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class Members have been adversely affected and damaged in that Defendant failed to adequately protect their PII to the detriment of Plaintiffs and the Class.

43. *Adequacy of Representation*: Plaintiffs will fairly and adequately represent the Class because they have the Class Members' best interests in mind, their individual claims are co-extensive with those of the Class, and they are represented by qualified counsel experienced in class action litigation of this nature.

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

45. The Class may be certified pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure because Defendant has acted on grounds generally applicable to the Class, thereby

making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

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

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

COUNT I

NEGLIGENCE

(Brought on Behalf of Nationwide Class)

48. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

49. Defendant owed a duty of care to Plaintiffs and Class Members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of their systems.

50. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII provided to them by Plaintiffs and Class Members, thus resulting in unauthorized third party access to the Plaintiffs' and Class Members' PII.

51. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies,

procedures, and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII within their possession, custody, and control.

52. As a direct and proximate cause of failing to use appropriate security practices, Plaintiffs' and Class Members' PII was disseminated and made available to unauthorized third parties.

53. Defendant admitted that Plaintiffs' and Class Members' PII was wrongfully disclosed as a result of the breach.

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

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

56. Neither Plaintiffs nor Class Members contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have been put at an increased risk of credit fraud or identity theft and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiffs and Class Members for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiffs and Class Members to the extent that they have directly sustained damages as a result of identity theft or other

unauthorized use of their PII, including the amount of time Plaintiffs and the Class Members have spent and will continue to spent as a result of Defendant's negligence. Defendant is also liable to Plaintiffs and Class Members to the extent their PII has been diminished in value and that Plaintiffs and Class Members no longer control that PII and to whom it would be disseminated.

COUNT II

NEGLIGENCE PER SE

(Brought on Behalf of Nationwide Class)

57. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

58. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

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

60. Defendant solicited, gathered, and stored PII of Plaintiffs and the Class Members to facilitate transactions which affect commerce.

61. Defendant violated the FTCA by failing to use reasonable measures to protect PII of Plaintiffs and the Class Members and not complying with applicable industry standards, as described herein.

62. Defendant's violation of the FTCA constitutes negligence per se.

63. Plaintiffs and the Class Members are within the class of persons that the FTCA was

intended to protect.

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

65. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class Members have suffered, and continue to suffer, damages arising from the breach.

COUNT III

BREACH OF IMPLIED CONTRACT

(Brought on Behalf of Nationwide Class)

66. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

67. When Plaintiffs and Class Members provided their PII to Defendant, they entered into implied contracts by which Defendant agreed to protect their PII.

68. Defendant invited applicants, including Plaintiffs and the Class Members, to use their portal.

69. An implicit part of the offer was that Defendant would safeguard the PII using reasonable or industry-standard means.

70. Based on the implicit understanding and also on Defendant's representations, Plaintiffs and the Class Members accepted the offers and provided Defendant their PII by using the portal.

71. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII as promised.

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

73. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII.

74. The losses and damages Plaintiffs and Class Members sustained described herein were the direct and proximate result of Defendant's breaches of their implied contracts with them.

COUNT IV

INVASION OF PRIVACY

(Brought on Behalf of Nationwide Class)

75. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

76. Defendant invaded Plaintiffs' and the Class Members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class Members' PII and by negligently maintaining the confidentiality of Plaintiffs' and Class Members' PII, as set forth above.

77. The intrusion was offensive and objectionable to Plaintiffs, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and Class Members' PII was disclosed without prior written authorization of Plaintiffs and the Class.

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

79. As a proximate result of Defendant's above acts, Plaintiffs' and the Class Members'

PII was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class Members suffered damages.

80. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class Members' PII with a willful and conscious disregard of Plaintiffs' and the Class Members' right to privacy.

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

COUNT V

DECLARATORY RELIEF

(Brought on Behalf of Nationwide Class)

82. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

83. Pursuant to the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq*., Plaintiffs and Class Members request the Court to enter a judgment declaring, *inter alia*, (i) Defendant owed (and continues to owe) a legal duty to safeguard and protect Plaintiffs' and Class Members' PII, (ii) Defendant breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class Members' PII, and (iii) Defendant's breach of their legal duties directly and proximately caused the breach, and the resulting damages, injury, and harm suffered

by Plaintiffs and Class Members.

COUNT VI

UNJUST ENRICHMENT

(Brought on Behalf of Nationwide Class)

84. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

85. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiffs' and Class Members' PII.

86. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class Members.

87. Nevertheless, Defendant continued to obtain the benefits conferred on them by Plaintiffs and Class Members.

88. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resultant breach disclosing Plaintiffs' and Class Members' PII, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms of, *inter alia*, attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

89. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiffs and Class Members, wherein it profited from interference with Plaintiffs' and Class Members'

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

90. Accordingly, Plaintiffs, on behalf of themselves and the Class, respectfully requests this Court award relief in the form of restitution and/or compensatory damages.

COUNT VII

INJUNCTIVE RELIEF

(Brought on Behalf of Nationwide Class)

91. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

92. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and resulting security breach have caused (and will continue to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of, *inter alia*, (i) identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy and PII, (iv) breach of the confidentiality of their consumer reports and consumer credit information, (v) deprivation of the value of their consumer credit information, for which there is a well-established national and international market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

93. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Defendant to (i) notify each person whose consumer credit information was exposed in the security breach, (ii) provide credit monitoring to each such person for a reasonable period of time, substantially in excess of

one year, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (*i.e.*, data breach insurance), and (iv) discontinue its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and resulting security breach.

94. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendant to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's computer systems on a periodic basis, (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) conducting regular database scanning and security checks, (v) regularly evaluating web applications for vulnerabilities to prevent web application threats, and (vi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain data security lapses.

95. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury in the event Defendant commits another security lapse, the risk of which is real, immediate, and substantial.

96. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant suffers another massive security lapse, Plaintiffs and Class Members will likely again incur millions of dollars in damages. On the other hand, and setting aside the fact that Defendant has a

pre-existing legal obligation to employ adequate data security measures, Defendant's cost to comply with the above-described injunction it is already required to implement is relatively minimal.

97. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another security lapse, thereby eliminating the damages, injury, and harm that would be suffered by Plaintiffs, Class Members, and the numerous future applicants whose confidential and sensitive PII would be compromised.

COUNT VIII

BAILMENT

(Brought On Behalf of Nationwide Class)

98. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 47.

99. Plaintiffs and Class Members provided, or authorized disclosure of, their PII to Defendant for the exclusive purpose of applying for unemployment benefits and using the associated portal.

100. In allowing their PII to be made available to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard their PII.

101. For its own benefit, Defendant accepted possession of Plaintiffs' and Class Members' PII for the purpose of making available its own services.

102. By accepting possession of Plaintiffs' and Class Members' PII, Defendant understood that Plaintiffs and Class Members expected Defendant to adequately safeguard their personal information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal

information.

103. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' personal information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class Members' PII.

104. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs and Class Members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth above.

105. As a direct and proximate result of Defendant's breach of its duties, the personal information of Plaintiffs and Class Members entrusted, directly or indirectly, to Defendant during the bailment (or deposit) was damaged and its value diminished.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, for themselves and Class Members, respectfully request that:

(i) this action be certified as a class action;

(ii) Plaintiffs be designated Class Representatives; and

(iii) Plaintiffs' counsel be appointed as Class Counsel.

Plaintiffs, for themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Defendant, in Plaintiffs' favor for:

(i) compensatory and punitive damages in an amount to be determined by the trier of fact;

(ii) declaratory and injunctive relief (as set forth above);

(iii) attorneys' fees, litigation expenses, and costs of suit incurred through the trial and any appeals of this case;

(iv) pre- and post-judgment interest on any amounts awarded; and

(v) such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiffs, individually and on behalf of Class Members, respectfully demand a trial by jury on all of his claims and causes of action so triable.

Dated: May 21, 2020

Respectfully Submitted,

/s/Amanda Peterson

Amanda Peterson (AP1797)
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
212-564-4568
apeterson@forthepeople.com

John A. Yanchunis
(*Pro Hac Vice* application forthcoming)
Ryan J. McGee
(*Pro Hac Vice* application forthcoming)
MORGAN & MORGAN
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
813-275-5272
JYanchunis@ForThePeople.com
RMcGee@ForThePeople.com

Jeffrey S. Goldenberg
(*Pro Hac Vice* applications forthcoming)
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: 513-345-8297
Fax: 513-345-8294
jgoldenberg@gs-legal.com

Joseph M. Lyon
(*Pro Hac Vice* application forthcoming)
The Lyon Firm, P.C.
2754 Erie Ave
Cincinnati, Ohio 45208
(513) 381-2333
jlyon@thelyonfirm.com

Charles E. Schaffer, Esquire
(*Pro Hac Vice* application forthcoming)

Levin Sedran & Berman
Counselors at Law and Proctors in Admiralty
510 Walnut Street, Suite 500
Philadelphia, PA 19106
(215) 592-1500, Fax 592-4663
CSchaffer@lfsblaw.com

Gary E. Mason
(*Pro Hac Vice* application forthcoming)
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue, NW, Suite 305
Washington, D.C. 20016
d 202.640.1160 m 202.256.1169 |
gmason@masonllp.com

Attorneys for Plaintiffs and the Putative Class