UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF NEW YORK

JANET M. BURNS, individually and on behalf of other similarly situated persons, Plaintiff, vs. DELOITTE CONSULTING LLP, Defendant	Case No. 1:20-cv-4077 **CLASS ACTION COMPLAINT** **Jury Demand**

Plaintiff Janet M. Burns ("Plaintiff"), by and through her undersigned attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Deloitte Consulting LLP ("Deloitte" or "Defendant") and makes the following allegations based upon knowledge as to herself and her own acts, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to implement and maintain reasonable security measures over personally identifiable information (the "Personal Information" or "PI") entrusted to it—in particular, her name, address, and Social Security number.

2. In connection with the federal Pandemic Unemployment Assistance program, Deloitte contracts with state agencies—including the Ohio Department of Job and Family Services ("ODJFS"), the Illinois Department of Employment Security ("IDES"), the Colorado Department of Labor and Employment ("CDLE"), and the Arkansas Division of Workforce Services ("ADWS")—to create and maintain web-portals by which applicants may apply for benefits and communicate with the state agencies.

3. Plaintiff applied for unemployment benefits through ODJFS' online portal.

4. On May 20, 2020, ODJFS sent a letter to Plaintiff notifying her that Deloitte had discovered on May 15, 2020 that the web-portal it created and maintained exposed applicants' Personal Information to the public. The letter further urged Plaintiff to consider "obtaining a copy of [her] credit report] or having "a fraud alert placed on [her] consumer credit file." In May 2020, IDES, CDLE, and ADWS publicly confirmed that Deloitte's web-portal similarly exposed the Personal Information of applicants in their states as well.

5. On information and belief, Deloitte's web-portals exposed hundreds of thousands of applicants' Personal Information to the public.

6. Criminals use information like the Personal Information to commit crimes, such as opening fraudulent credit accounts in the name of the victim, filing a fraudulent income tax return and diverting any refund to the criminal's bank account, and impersonate the victim when arrested, when obtaining medical services, and seeking employment. These crimes cause significant harm to the victims that can last for years, particularly where information as sensitive and valuable as Social Security numbers are involved.

7. The Data Breach was caused and enabled by Deloitte's violation of its common law and statutory obligations to implement and maintain reasonable security measures to protect Personal Information from unauthorized access, acquisition, destruction, use, and modification.

II. PARTIES

8. Plaintiff Janet M. Burns is an adult who resides in Seven Hills, Ohio. Plaintiff applied for unemployment benefits through the web-portal created and maintained by Deloitte, and her Personal Information was left publicly accessible. As a result of Defendants' failures to adequately safeguard Plaintiff's Personal Information, Plaintiff has been put at risk of fraudulent transactions and other substantial harms.

9. Defendant Deloitte Consulting LLP is organized under Delaware law and is 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.

III. JURISDICTION AND VENUE

10. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 because Plaintiff's claims arise under federal law and § 1332(d), as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000,

exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

11. This Court has personal jurisdiction over Deloitte because it maintains its headquarters in the forum state, is authorized to do business in this District and regularly conducts business in this District, and has sufficient minimum contacts with this state and/or sufficiently avails itself of the markets of this state through its promotion, sales, and marketing within this state to render the exercise of jurisdiction by this Court permissible. In addition, the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated in part from this District.

12. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendant is a resident of and/or does business in this District, has intentionally availed itself of the laws and markets within this District by conducting substantial business in this District, and a significant portion of the facts and circumstances giving rise to this Complaint occurred in or emanated from this District.

IV. FACTUAL ALLEGATIONS

A. Background.

13. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act established the Pandemic Unemployment Assistance ("PUA") program. The PUA expands unemployment insurance eligibility to self-employed workers, freelancers, independent contractors, and part-time contractors impacted by the 2020 COVID-19 outbreak.

14. Deloitte regularly assists state agencies with unemployment insurance solutions, such as claim services, benefit payments, control, reporting services, administrative services, and document management services.

15. The PUA program required a new processing system, so several state agencies contracted with Deloitte to design and maintain a portal system.

16. To apply for PUA benefits, applicants must submit sensitive Personal Information, such as their name, address, and social security number. Deloitte knew that applicants through its web-portals entrusted it with sensitive Personal Information and that safeguarding such information was vitally important.

17. The web-portal Deloitte designed was activated on or around May 11, 2020.

B. The Data Breach.

18. On May 15, 2020, Illinois State Representative Terri Bryant notified Illinois Governor J.B. Pritzker that one of her constituents had found a spreadsheet on the IDES portal containing the Personal Information of "thousands of unemployment applicants."[1] On May 17, 2020, IDES officials confirmed that applicants' Personal Information had been publicly exposed.

19. On May 15, 2020, ADWS confirmed that its PUA system that applicants' Personal Information, including social security numbers, bank account and routing numbers, and other sensitive information, had been exposed to the public.

20. On May 18, 2020, CDLE confirmed that its PUA system also left applicants' Personal Information publicly accessible.

[1] https://repbryant.com/2020/05/16/rep-bryant-demands-governor-answer-questions-involving-potential-massive-ides-unemployment-applicant-data-breach/

21. On May 20, 2020, ODJFS sent applicants an email notifying them that the PUA system Deloitte designed and maintained had exposed applicants' Personal Information to the public.

22. Plaintiff became aware of the Data Breach after he received the email from ODJFS.

23. On information and belief, Deloitte's substandard security practices directly and proximately caused the public exposure of hundreds of thousands of Americans' Personal Information.

24. On information and belief, Deloitte failed to detect the public exposure of applicants' information because it failed to adhere to commonly accepted industry security standards.

25. Plaintiff and Class Members have been damaged as a direct and proximate result of Deloitte's failure to protect their Personal Information.

26. Plaintiff and Class members have suffered injury and damages, including actual identity theft and fraud, an increased risk of identity theft and identity fraud, improper disclosure of their PI, the time and expense necessary to mitigate, remediate, and sort out the identity theft and identity fraud and increased risk of identity theft and identity fraud, and a deprivation of the value of their Personal Information.

27. Plaintiff and Class members have suffered and will continue to suffer additional damages based on the opportunity cost and time Plaintiff and Class members are forced to expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

C. Industry standards, identity theft, and protection of personal information.

28. It is well known that PI, and financial account information in particular, is an invaluable commodity and a frequent target of hackers. Despite this widespread knowledge and industry alerts of other notable data breaches, Defendant failed to take reasonable steps to adequately protect its systems from being breached.

29. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[2]

30. Defendant is, and at all relevant times has been, aware that the PI it maintains is highly sensitive and could be used for illegal purposes by third parties.

31. Consumers place a high value not only on their PI, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[3]

32. Consumers are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[4] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security

---

[2] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

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

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

Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[5]

33. In light of the multiple high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, and Equifax, Defendant is, or reasonably should have been, aware of the importance of safeguarding its customers' PI, as well as of the foreseeable consequences of its systems being breached.

34. Nonetheless, Defendant failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

35. Defendant had a duty to Plaintiff and Class members to properly secure their PI, encrypt, tokenize, and maintain their PI using industry standard methods, use widely available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class members, and promptly notify Plaintiff and Class members when Defendant became aware of the potential that their customers' PI may have been compromised.

V. CLASS ACTION ALLEGATIONS

36. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and a Nationwide Class defined as (the "Class"):

> All persons whose Personal Information was compromised in the PUA portal data breach.

37. **Numerosity.** Class Members are so numerous that joinder of individual claims is impracticable. Based on public information, hundreds of thousands of individuals have filed for

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

unemployment through Deloitte's portal, so hundreds of thousands of affected individuals are likely to submit claims.[6] Class Members can be easily identified through Defendant's records.

38. **Commonality and predominance.** Common questions of law and fact exist as to all Class members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

a. Whether Defendant engaged in wrongful conduct as alleged herein;

b. Whether Defendant owed a duty to Plaintiff and Class members to adequately protect their Personal Information and to provide timely and accurate notice of the Data Breach to Plaintiff and Class members, and whether Defendant willfully, recklessly, or negligently breached these duties;

c. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures to prevent unauthorized access to its data security networks and to Plaintiff and Class members' Personal Information;

d. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

e. Whether Defendant failed to inform Plaintiff and Class members of the Data Breach in a timely and accurate manner;

f. Whether Defendant continues to breach its duties to Plaintiff and Class members;

---

[6] Since March 14, 2020, there have been: 407,561 applications in Colorado, 1,039,231 applications in Illinois, and 1,219,870 applications in Ohio. https://www.nbcnews.com/business/economy/unemployment-claims-state-see-how-covid-19-has-destroyed-job-n1183686 (last accessed May 22, 2020).

g. Whether Defendants have sufficiently addressed or remedied Plaintiff's and Class members' injuries and have taken adequate preventive and precautionary measures to ensure that Plaintiff and Class members will not experience further harm;

h. Whether Defendants engaged in unfair or deceptive practices by failing to disclose that they failed to properly safeguarded Plaintiff's and Class members' Personal Information;

i. Whether Defendants violated the consumer protection statutes applicable to Plaintiff and members of the Class;

j. Whether Plaintiff and Class members suffered damages as a proximate result of Defendants' conduct or failure to act; and

k. Whether Plaintiff and Class members are entitled to damages, equitable relief, and other relief.

39. **Typicality.** Plaintiff's claims are typical of the claims of the Class he seeks to represent. He, like all Class Members, has suffered harm as a result of Defendant's failure to adequately protect her Personal Information.

40. **Adequacy.** Plaintiff will fairly and adequately protect the interests. She has no interests adverse to any class members, and he is represented by qualified counsel experienced in class action litigation.

41. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class member, while meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class members could afford individual litigation, the judicial system could not. In addition to the burden and expense

of managing many actions arising from the Data Breach, individual litigation increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

42. In the alternative, the proposed classes may be certified because:

a. the prosecution of separate actions by the individual members of the Class would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendant;

b. the prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class members, or which would substantially impair their ability to protect their interests; and

c. Defendant acted or refused to act on grounds generally applicable to the proposed class, thereby making appropriate final and injunctive relief with respect to members of the Class as a whole.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
15 U.S.C. §§ 1681 *ET SEQ.*

43. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

44. One of the fundamental purposes of the FCRA is to protect consumers' privacy. 15 U.S.C. § 1681(a). Protecting consumers' privacy involves adopting reasonable procedures to keep sensitive information confidential. 15 U.S.C. § 1681(b). The FCRA defines a "consumer reporting agency" as

> any person, which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information or consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

45. The FCRA defines a "consumer report" as:

> any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under 15 U.S.C. § 16881(b).

46. Defendant regularly assembles consumer information including, among other things, financial and credit information, such as names, dates of birth, and social security numbers. Defendant also regularly uses interstate commerce to furnish this type of consumer information to third parties.

47. Plaintiff's and Class members' PI constitutes consumer reports under FCRA, because this information bears on, among other things, their creditworthiness, credit standing, credit capacity, character, general reputation, financial information, and personal characteristics, and it is used or collected, at least in part, for the purpose of establishing Plaintiff's and Class members' eligibility for credit to be used primarily for personal, family, or household purposes, and for establishing relevant rates.

48. FCRA requires the adoption of reasonable procedures with regard to, *inter alia*, the confidentiality and proper utilization of personal information. 15 U.S.C. § 1681(b). FCRA also requires that consumer reporting agencies "maintain reasonable procedures designed to . . .

limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e.

49. Defendant's failure to adequately protect and safeguard Plaintiff's and Class members' PI resulted in the disclosure of their personal information to one or more third parties in violation of FCRA because the disclosure was not necessary to carry out the purposes for which Defendant received the information, and it was not permitted by statute, regulation or order. Defendant's violations of FCRA were willful or, at the very least reckless, constituting willfulness.

50. As a direct and proximate result of Defendant's willful or reckless failure to adopt and maintain reasonable procedures to limit the furnishing and disclosure of Plaintiff's and Class members' PI to the purposes listed in the statute, Plaintiff's and Class members' PI was disclosed and disseminated to unauthorized third parties. Plaintiff and Class members have suffered injury and harm and will continue to suffer injury and harm because of Defendant's conduct.

51. As a further direct or proximate result of Defendant's willful or reckless FCRA violations, as described above, Plaintiff and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the harms and damages described in this Complaint.

52. Accordingly, Plaintiff and Class members are entitled to compensation for their actual damages in an amount to be determined at trial or statutory damages of not less than $100, and not more than $1,000, each, as well as attorneys' fees, punitive damages, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a). Plaintiff also seeks injunctive relief

enjoining the above described wrongful acts and practices of Defendant and requiring Defendant to employ and maintain industry accepted standards for data security and privacy.

SECOND CAUSE OF ACTION
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
15 U.S.C. §§ 1681 *ET SEQ*.

53. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the Class against Defendant.

54. Defendant obtained sensitive Personal Information from Plaintiff and Class members in providing financial account and credit services.

55. Defendant owed a duty to Plaintiff and Class members to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their Personal Information from being compromised by unauthorized persons. This duty included, *inter alia*, designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class members' Personal Information was adequately protected both in the process of collection and after collection.

56. Defendant also owed a duty to Plaintiff and Class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks adequately protected Plaintiff's and Class members' Personal Information.

57. Defendant holds itself out as an expert in compliance, and thus knew or should have known the risks inherent in collecting and storing Personal Information and the critical importance of provide adequate security for that information.

58. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class members. This conduct included but was not limited to Defendant's failure to take reasonable steps and opportunities to prevent and stop the Data Breach. Defendant's conduct also included

its decision not to comply with industry standards for the safekeeping and maintenance of Plaintiff's and Class members' Personal Information.

59. Defendant knew or should have known that it had inadequate data security practices to safeguard such information.

60. Defendant breached its duties to Plaintiff and Class members by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class members' Personal Information. Defendant's breach of its duties proximately caused the injuries and damages Plaintiff and Class members have suffered.

61. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members suffered injury and are entitled to damages in an amount to be proven at trial. Defendant violated its duties of care with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

THIRD CAUSE OF ACTION
BREACH OF CONTRACT

62. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

63. When Defendant and the various state governments entered into contracts to provide Plaintiff and Class Members with benefits under the PUA and program, they intended to provide financial and other benefits to Plaintiff and Class Members. As a result, Defendant received taxpayer funds through the CARES Act and was required to be provided Plaintiff's and Class Members' Personal Information, which they were obligated by law to keep confidential. Accordingly, Plaintiff and Class Members were third-party beneficiaries under the contracts between the government and Defendant.

64. Plaintiff and Class Members would not have provided their Personal Information to Defendant if they knew Defendant would not safeguard their Personal information as promised.

65. Defendant violated the contracts by failing to employ reasonable and adequate privacy practices and measures, leading to the disclosure of Plaintiff's and Class members' PI for purposes not required or permitted under the contracts or the law.

66. Plaintiff and Class members have been damaged by Defendant's conduct by incurring the harms and injuries arising from the Data Breach now and in the future.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

67. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

68. When Plaintiff and Class Members provided their Personal Information to Defendant, they entered into implied contracts by which Defendant agreed to protect their Personal Information.

69. Defendant invited applicants, including Plaintiffs and Class members, to use their portal.

70. An implied term of Defendant's offer was that Defendant would safeguard Personal Information using reasonable or industry-standard means.

71. Plaintiff and Class Members would not have provided their Personal Information to Defendant if they knew Defendant would not safeguard their Personal information as promised.

72. Defendant violated the contracts by failing to employ reasonable and adequate privacy practices and measures, leading to the disclosure of Plaintiff's and Class members' PI for purposes not required or permitted under the contracts.

73. Plaintiff and Class members have been damaged by Defendant's conduct by incurring the harms and injuries arising from the Data Breach now and in the future.

FIFTH CAUSE OF ACTION
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

74. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

75. As described above, Plaintiff and Class Members were third-party beneficiaries under the contracts between Defendant and the government and also maintained an implied contract with Defendant when they provided their Personal Information.

76. Inherent in every contract is that implied covenant of good faith and fair dealing, which Defendant violated by failing to maintain reasonable data security protocols, leading to the disclosure of Plaintiff's and Class members' PI for purposes not required or permitted under the contracts.

77. Plaintiff and Class members have been damaged by Defendant's conduct by incurring the harms and injuries arising from the Data Breach now and in the future.

SIXTH CAUSE OF ACTION
NEGLIGENCE

78. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

79. Plaintiff and Class members entrusted Defendant with highly sensitive and personal private data subject to confidentiality.

80. In obtaining and storing Plaintiff's and Class members' Personal Information, Defendant owed a duty of reasonable care in safeguarding this PI.

81. Defendant's networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class members' Personal Information was secured from release, disclosure, and/or publication.

82. Defendants' networks, systems, protocols, policies, procedures and practices were not reasonable given the sensitivity of the Plaintiff's and Class member's PI.

83. Upon learning of the Data Breach, Defendants should have immediately reported the Data Breach to Plaintiff and Class members, credit reporting agencies, the Internal Revenue Service, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiff and Class members.

84. Despite knowing their networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class members' PI were secured from release, disclosure, and publication, Defendant ignored the inadequacies and were unmindful of the risk of release, disclosure, and publication it had created.

85. Defendant's behavior evidences a reckless disregard for Plaintiff's and Class members' rights. Defendant's negligence is directly linked to Plaintiff's and Class members' injuries.

86. As a result of Defendant's reckless disregard for Plaintiff's and Class members' rights by failing to secure their Personal Information despite knowing their networks, systems, protocols, policies, procedures, and practices were not adequately designed, implemented,

maintained, monitored, and tested, Plaintiff and Class members suffered injury, including but not limited to the impermissible release, disclosure, and publication—both directly and indirectly by Defendant as well as unauthorized parties—of their Personal Information as well as exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Indeed, Plaintiff himself has actually suffered such harm already. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently. Plaintiff and Class members have also incurred and will continue to incur costs for the time and expense necessary to obtain credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The impermissible release, disclosure, and publication of Plaintiff's and Class members' PI has also diminished the value of their PI.

87. The harm to Plaintiff and the Class members was a proximate and reasonably foreseeable result of Defendant's breach of its duty of reasonable care in safeguarding Class members' Personal Information.

88. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
NEGLIGENCE PER SE

89. Plaintiffs incorporate the above allegations by reference.

90. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses of failing to use reasonable measures to protect data collected on consumers. The FTC publications and orders described above also form and inform the basis of Defendant's duty.

91. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to Plaintiffs and the other Class members.

92. Defendant's violation of Section 5 of the FTCA constitutes negligence per se.

93. Plaintiffs and the other Class members are within the class of persons that the FTCA was intended to protect.

94. The harm that occurred as a result of the Data Breach is the type of harm that 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 security measures and avoid unfair or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class Members as a result of the Data Breach.

95. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendant's violations of the FTC Act and similar state statutes. Plaintiffs and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

EIGHTH CAUSE OF ACTION
INVASION OF PRIVACY

96. Plaintiff incorporates all previous allegations by reference

97. Defendant invaded Plaintiff's and the Class Members' right to privacy by allowing the unauthorized access to Plaintiff's and Class Members' Personal Information and by negligently maintaining the confidentiality of Plaintiffs' and Class Members' Personal Information, as set forth above.

98. The intrusion was offensive and objectionable to Plaintiff, the Class Members, and any reasonable person of ordinary sensibilities.

99. The intrusion was into a place or thing which was private and is entitled to be private.

100. As a proximate result of Defendant's above acts, Plaintiff's and the Class Members' Personal Information was viewed, distributed, and used by persons without written authorization, thereby causing them damages.

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

102. Unless and until enjoined and restrained by court order, Defendant's wrongful conduct will continue to cause Plaintiff and the Class Members great and irreparable injury as the Personal Information maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons.

103. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damage will not end the invasion of privacy for Plaintiff and the Class.

NINTH CAUSE OF ACTION
BAILMENT

104. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

105. Plaintiff and Class members provided, or authorized disclosure of, their PI to Defendant for the exclusive purpose of applying for unemployment benefits and using the associated portal.

106. In allowing their PI to be made available to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard their PI.

107. For its own benefit, Defendant accepted possession of Plaintiff's and Class Members' PI for purpose of making available its own service.

108. Defendant understood that Plaintiff and Class Members expected Defendant to adequately safeguard their personal information. Accordingly, a bailment was established for the parties' mutual benefit. During the bailment, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care, diligence, and prudence in protect their PI.

109. Defendant breached its duty of care by failing to take appropriate measures to safeguard Plaintiff's and the Class Member's PI, resulting in the unauthorized disclosure of their PI.

110. As a direct and proximate result of Defendant's breach of its duty, Plaintiff and Class Members suffered damages that were reasonably foreseeable to Defendant.

111. As a direct and proximate result, the PI Plaintiff and the Class Members entrusted to Defendant during the bailment was damaged and its value diminished.

TENTH CAUSE OF ACTION
BREACH OF CONFIDENCE

112. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

113. As alleged above, Plaintiff and Class Members had agreements with Defendant, both express and implied, that required Defendant to keep their PI confidential.

114. Defendant breached that confidence by disclosing Plaintiff's and Class Members' PI without their authorization and for unnecessary purposes.

115. As a result of the Data Breach, Plaintiff and Class Members suffered damages that were attributable to Defendant's failure to maintain confidence in their PI.

ELEVENTH CAUSE OF ACTION
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW, SECTION 349

116. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

117. New York's General Business Law, Section 349, prohibits "[d]eceptive acts and practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." Violations of Section 349 are unlawful an actionable by aggrieved consumers.

118. At all times herein, Defendant was subject to the requirements of Section 349, which it breached in connection with the data breach associated with the PUA program which was intended to provide services in the furnishing of CARES Act benefits to consumers and the public at large.

119. Defendant violated Section 349 by disclosing Plaintiff's and Class Members' PI in connection with the PUA data breach.

120. As a result of the Data Breach, Plaintiff and Class Members suffered damages that were attributable to Defendant's failure to maintain the confidentiality in their PI. Accordingly,

pursuant to Section 349(h), Plaintiff and Class Members are entitled to actual damages, statutory damages, injunctive relief, attorneys' fees and costs of suit.

TWELFTH CAUSE OF ACTION
DECLARATORY JUDGMENT

121. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

122. Defendants failed to fulfill their obligations to provide adequate and reasonable data security measures for the Personal Information of Plaintiff and the Class, as evidenced by the Data Breach.

123. As a result of the Data Breach, Defendant's systems are more vulnerable to access by unauthorized parties and require more stringent measures to be taken to safeguard the Plaintiff's and Class members' Personal Information going forward.

124. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide data security measures that will adequately protect Plaintiff's and Class members' Personal Information.

125. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent, industry-standard data security practices to provide reasonable protection and security to Plaintiff and Class members' Personal Information. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with their obligations, and that Defendant must implement and maintain reasonable data security measures on behalf of Plaintiff and the Class to comply with its data security obligations.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and on behalf of the Class, prays for relief as follows:

A. For an order certifying the Class and appointing Plaintiff as class representative;

B. Awarding monetary and actual damages and/or restitution, as appropriate;

C. Awarding punitive damages, as appropriate;

D. Awarding declaratory and injunctive relief as permitted by law or equity to ensure that the Class has an effective remedy, including enjoining Defendant from continuing its unlawful practices;

E. Prejudgment interest to the extent allowed by the law;

F. Awarding all costs, including expert fees and attorneys' fees, expenses, and costs of prosecuting this action; and

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

VIII. JURY TRIAL DEMAND

Plaintiff, individually and on behalf of all others similarly situated, demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 27 day of May, 2020.

By: s/ *Laurence D. King*
Laurence D. King

Laurence D. King (S.D.N.Y. Bar No. LK7190)
Matthew B. George (*pro hac vice to be filed*)
KAPLAN FOX & KILSHEIMER LLP
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: (415) 772-4700
Email: *lking@kaplanfox.com*
mgeorge@kaplanfox.com

David A. Straite (S.D.N.Y. Bar No. DS0114)
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue
New York, NY 10022-7237
Telephone: (212) 687-1980
Email: *dstraite@kaplanfox.com*

David P. Meyer, Esq.
Matthew R. Wilson, Esq.
Michael J. Boyle, Jr., Esq.
(*pro hac vice* motions to be filed)
MEYER WILSON CO. L.P.A.
1320 Dublin Road, Suite 100
Columbus, OH 43215
Phone: (614) 224-6000
Facsimile: (614) 224-6066