UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Melissa Alexander, on behalf of herself and all others similarly situated, Plaintiff, v. Deloitte Consulting, LLP, Defendant.	Case No. 1:20-cv-04129 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Melissa Alexander ("Plaintiff") brings this class action against Defendant Deloitte Consulting, LLP ("Deloitte" or "Defendant"). Plaintiff makes the following allegations upon personal knowledge as to her own acts, and upon information and belief, and the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. In the wake of the COVID-19 pandemic, Defendant contracted with various state agencies—including the Ohio Department of Job and Family Services, the Illinois Department of Employment Security, and the Colorado Department of Labor and Employment—to help states administer the federal Pandemic Unemployment Assistance ("PUA") program by designing, building, and maintaining web-based portals through which individuals may apply for unemployment benefits and communicate with state officials.

2. Defendant failed to take reasonable and adequate measures to secure the personally identifiable information ("PII") of Plaintiff and similarly situated individuals (the class members, as defined below) in the course of designing, building, and maintaining computerized unemployment systems for multiple state agencies.

3. Because of Defendant's failure to exercise due care, members of the public were able to access unemployment applicants' PII, including social security numbers. As a result, Plaintiff and the class members have been injured through the loss of control of their PII, the need to take appropriate steps to mitigate their injury, and the heightened and imminent risk of identity theft or fraud.

PARTIES

4. Plaintiff Melissa Alexander is a resident of Blacklick, Ohio. She filed a claim for unemployment benefits on May 13, 2020, through the PUA portal available to Ohio residents. On May 20, 2020, she received an email from the Ohio Department of Job and Family Services advising that her "name, Social Security number, and street address pertaining to [her] application for receipt of unemployment compensation benefits" were compromised and made available to other unemployment applicants.

5. Defendant Deloitte Consulting, LLP, is a Delaware limited liability company with its principal place of business located at 30 Rockefeller Plaza, New York, NY 10112.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction because this is a class action, the matter in controversy exceeds $5 million (exclusive of interest and costs), and there is minimal diversity. 28 U.S.C. § 1332(d)(2).

7. The Court has personal jurisdiction because Defendant is headquartered in this District.

8. Venue is proper because Defendant is headquartered in this District. 28 U.S.C. § 1391(b)(1).

FACTS

9. The PUA program provides expanded unemployment benefits to workers affected by COVID-19.[1]

10. Unemployment benefits are provided and administered by state governments.

11. Some state governments, including at least Ohio, Illinois, and Colorado, contracted with Defendant for its ability to provide public sector labor and employment services, including unemployment insurance solutions such as claims services, wage determinations, benefit payments control, reporting services, administrative services, and document management services.[2]

12. In designing, building, maintaining, and operating PUA portals, Defendant was entrusted with unemployment applicants' PII, including that of Plaintiff and the absent class members.

13. Defendant assumed a duty to keep unemployment applicants' PII secure.

14. Defendant knew that safeguarding unemployment applicants' PII is critically important because of the harm flowing from a compromise of that data. Indeed, the U.S. Federal Trade Commission ("FTC") publishes a guide for businesses about protecting PII.[3]

15. Defendants' cloud-based PUA portal went live on approximately May 11, 2020, despite lacking appropriate safeguards to protecting unemployment applicants' PII.

---

[1] U.S. Dep't of Labor, U.*S. Dep't of Labor Publishes Guidance on Pandemic Unemployment Assistance*, Apr. 5, 2020, https://www.dol.gov/newsroom/releases/eta/eta20200405 (last visited May 26, 2020).

[2] Deloitte, *Public Sector Labor and Employment services | uFACTS*, https://www2.deloitte.com/us/en/pages/public-sector/solutions/unemployment-insurance-services.html (last visited May 26, 2020).

[3] FTC, *Protecting Personal Information: A Guide for Business*, Oct. 2016, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited May 26, 2020).

16. On May 16, 2020, Illinois acknowledged a "glitch" in Defendant's PUA system that "made some private information publicly available."[4] Although the exact number of Illinois residents affected by this data breach has not been publicly disclosed, 44,000 workers applied for unemployment benefits using Defendant's PUA portal on the first day it was available. The number of applicants since that time is likely substantially higher.

17. On May 19, 2020, Colorado acknowledged "a limited and intermittent data access issue," by which unemployment applicants were granted access to other applicants' private correspondence with the state—which included social security numbers.[5] A reported 72,000 individuals were affected in this manner.

18. Ohio acknowledged, via emails to unemployment applicants, that information including social security numbers, names, and addresses "inadvertently had the capability to be viewed by other claims."[6] A reported 130,000 unemployment applicants were affected.[7]

---

[4] Dan Mihalopoulos et al., *"Glitch" in New Illinois Unemployment System Made Private Information Public*, WBEZ, May 16, 2020, https://www.wbez.org/stories/glitch-in-new-illinois-unemployment-system-made-private-information-public/22b1dd10-4d79-4ddd-b14c-799ecdaa3ca6 (last visited May 26, 2020).

[5] Joe Rubino, *72,000 on Pandemic Unemployment Assistance in Colorado Had Private Information Exposed*, Denver Post, May 19, 2020, https://www.denverpost.com/2020/05/19/colorado-pandemic-unemployment-assistance-informatoin-exposed-coroanvirus-covid/ (last visited May 26, 2020).

[6] Cheyenne Haslett, *Struggle of Unemployment Claimants Compounded by Data Breach*, ABC News, May 21, 2020, https://6abc.com/struggle-of-unemployment-claimants-compounded-by-data-breach/6201835/ (last visited May 26, 2020).

[7] Cornelius Frolick, *Security Problem Could Affect 130K Ohio Unemployment Seekers*, Dayton Daily News, May 20, 2020, https://www.daytondailynews.com/news/local/security-problem-could-affect-130k-ohio-unemployment-seekers/Gj1jHOSkbDZOYLG2elVT4L/ (last visited May 26, 2020).

19. Recognizing the harm associated with a data breach of this nature, Deloitte is offering 12 months of free credit monitoring to all PUA unemployment applicants in Ohio, Colorado, and Illinois.

20. Plaintiff became aware of this data security breach when she received an email from the Ohio Department of Job and Family Services on May 20, 2020. That email stated: "Deloitte discovered on May 15, 2020 that your name, Social Security number, and street address pertaining to your application for and receipt of unemployment compensation benefits inadvertently had the capability to be viewed by other unemployment claimants."

21. As a direct and proximate result of Defendant's inadequate data security practices—in particular, making communications through the PUA portal, including applicants' PII, publicly available to other applicants—Plaintiff and the class members have sustained a concrete injury.

22. Plaintiff and class members face a significant risk of identity theft and fraud and will likely incur additional out-of-pocket costs as part of reasonable efforts to mitigate identity theft or fraud. The information exposed in the data breach is the information needed to obtain unemployment benefits, apply for and obtain lines of credit, and engage in other credit-related or financial activities.

23. Plaintiff and class members will spend substantial amounts of time and expense monitoring their accounts to identify fraudulent or suspicious activity, canceling and reissuing cards, purchasing credit monitoring and identity theft prevention services, attempting to withdraw funds linked to accounts that have been compromised or frozen, removing withdrawal and purchase limits on accounts that have been frozen, communicating with financial institutions to dispute fraudulent charges, resetting automatic billing instructions, freezing and unfreezing credit

bureau account information, cancelling and resetting payment card information and automatic payments, and paying late fees and declined payment penalties as a result of failed automatic payments.

24. Plaintiff and class members have lost the value of their PII and the opportunity to control how it is used.

25. PII has value on the black market. This type of PII permits many types of fraud, including obtaining government benefits, filing a fraudulent tax return, or obtaining a false identity that can create a false work history or arrest record.[8]

26. Social security numbers are particularly problematic PII to lose control of because they are difficult to change, even for victims of a data breach. Changing a social security number is a process requiring evidence of continuing misuse and continuing harm, and yet even that may not alleviate a victim's problems because a new number does not guarantee a new credit profile that has been wiped clean of incorrect information caused by fraud (and even if it did, the consumer may lose the benefits of their accurate credit history).

CLASS ACTION ALLEGATIONS

27. Pursuant to Federal Rule of Civil Procedure Rule 23(b)(3), Plaintiff brings this lawsuit on behalf of herself and on behalf of the proposed nationwide class (the "Class") defined as follows:

> All persons residing in the United States whose PII was compromised as a result of the PUA portal data breach.

[8] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian Blog (Mar. 11, 2019), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 26, 2020).

28. Plaintiff also seeks certification of a proposed Ohio class (the "Ohio Class") pursuant to Rule 23(b)(3), defined as follows:

> All persons residing in Ohio whose PII was compromised as a result of the PUA portal data breach.

29. Excluded from the Class and Ohio Class are Defendant and any entities in which Defendant or its subsidiaries or affiliates have a controlling interest; Defendant's officers, agents, and employees; and all persons who make a timely election to be excluded from the Class and Ohio Class. Also excluded from the Class and Ohio Class are the judges and court personnel in this action and any members of their immediate family.

30. **Numerosity:** The members of the Class and Ohio Class are so numerous that joinder of all class members would be impracticable. Plaintiff reasonably believes that class members number in the hundreds of thousands of people based on information disclosed by Ohio, Illinois, and Colorado. The names and addresses of the class members are identifiable through documents Defendant maintains.

31. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual class members, including:

a. Whether Defendant owed a legal duty to Plaintiff and class members to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and class members to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant had an implied contractual obligation to use reasonable security measures in safeguarding the PII;

d. Whether Defendant breached its implied contractual obligation to use reasonable security measures in safeguarding the PII;

e. What security measures Defendant must use to comply with its implied contractual obligation and legal duty to safeguard PII;

f. Whether Defendant's security measures to protect its computer systems were reasonable in light of industry data security standards and recommendations;

g. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and class members' PII;

h. Whether Plaintiff's and class members' PII was accessed, exposed, compromised, or stolen;

i. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

j. Whether Plaintiff and class members are entitled to equitable relief, including, but not limited to, injunctive relief; and

k. Whether Plaintiff and class members are entitled to damages or other monetary relief, and the amount thereof.

32. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the class members. Similar or identical legal violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

33. **Typicality:** Plaintiff's claims are typical of class members' claims because, among other things, Plaintiff and class members were injured through Defendant's substantially uniform misconduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and class

members, and there are no defenses that are unique to Plaintiff's claims. Plaintiff's and class members' claims arise from the same operative facts and are based on the same legal theories.

34. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class and Ohio Class because her interests do not conflict with the interests of the other class members she seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation, including data privacy and data security practices litigation; and Plaintiff will prosecute this action vigorously for the benefits of the Class and Ohio Class. Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

35. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and class members is relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for class members to individually seek redress for Defendant's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

Negligence

36. Defendant owed a duty of care to Plaintiff and members of the Class and Ohio Class to use reasonable means to secure and safeguard the PII and to prevent its unauthorized access and disclosure.

37. Defendant's duty of care arises from Plaintiff and class members entrusting it with their PII, under common law principles.

38. Defendant also had a duty to provide adequate data security pursuant to the FTC Act, 15 U.S.C. § 45, which defines failure to use reasonably necessary measures to protect PII as a prohibited unfair practice in or affecting commerce.

39. Defendant breached its duty by failing to use security practices that would protect the PII provided to it by Plaintiff and class members, thereby resulting in unauthorized third-party access to the PII. Defendant failed to utilize and manage processes that would safeguard and protect Plaintiff and class members' PII.

40. As a direct and proximate result of Defendant's failure to use appropriate security practices, Plaintiff and class members' PII was made available to third parties.

41. The data breach caused direct and substantial damages to Plaintiff and class members.

42. Plaintiff and class members did not contribute to the breach or subsequent misuse of their PII.

43. On behalf of herself and the Class and Ohio Class, Plaintiff seeks actual and compensatory damages, in an amount to be proven at trial.

COUNT II

Breach of Implied Contract

44. When Plaintiff and members of the Class and Ohio Class provided their PII to Defendant, they entered into implied contracts by which Defendant agreed to protect their PII.

45. Defendant invited unemployment applicants, including Plaintiff and class members, to use its PUA portal.

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

47. Based on this understanding, Plaintiff and class members accepted this offer and provided Defendant their PII through the portal.

48. Plaintiff and class members would not have provided their PII had they known Defendant would not safeguard it as impliedly promised.

49. Plaintiff and class members fully performed their obligations under the implied contracts with Defendant.

50. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and class members' PII.

51. Defendant's breach of the implied contract caused direct and substantial damages to Plaintiff and class members.

52. On behalf of herself and the class, Plaintiff seeks actual and compensatory damages, in an amount to be proven at trial.

COUNT III

Unjust Enrichment

53. Defendant was enriched through its contracts with states, including Colorado, Illinois, and Ohio, by which it provided PUA portals and related services.

54. Defendant collected Plaintiff and Class members' and Ohio Class members' PII through those PUA portals.

55. Defendant saved costs it should have spent on ensuring the security of Plaintiff and class members' PII.

56. Defendant retained the benefit of the contracts it had with the states, and it retained Plaintiff and class members' PII, but it failed to provide and utilize adequate measures to protect the security of Plaintiff and class members' PII.

57. Under these circumstances, Defendant's retention of that benefit is unjust and violative of principles of equity and good conscience.

58. On behalf of herself and the class, Plaintiff seeks restitution, in an amount to be proven at trial.

PRAYER FOR RELIEF

59. Plaintiff, on behalf of herself and all others similarly situated, requests that the Court enter judgment as follows:

a. An order certifying the Class and Ohio Class, appointing Plaintiff as class representative, and appointing the undersigned counsel as class counsel;

b. Actual and compensatory damages, in an amount to be proven at trial;

c. Equitable disgorgement and restitution, in an amount to be proven at trial;

d. Pre- and post-judgment interest, to the full extent permitted by law;

e. Payment of reasonable attorneys' fees and costs; and

f. Any other relief that this Court deems just and proper.

DEMAND FOR JURY TRIAL

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

Dated: May 29, 2020

/s/ Katherine M. Aizpuru

Katherine M. Aizpuru (Bar No. 5305990)
kaizpuru@tzlegal.com
Hassan A. Zavareei*
hzavareei@tzlegal.com
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950

MELISSA S. WEINER*
weiner@pswlaw.com
JOSEPH C. BOURNE*
jbourne@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610

Jeff Ostrow*
ostrow@kolawyers.com
Jonathan M. Streisfeld*
streisfeld@kolawyers.com
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
1 West Las Olas Blvd. Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
Facsimile: (954) 525-4300

Attorneys for Plaintiff and the Proposed Class

* *Pro Hac Vice Forthcoming*