UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

GREG TORRANO, individually and on behalf of all others similarly situated, Plaintiff, vs. HORIZON ACTUARIAL SERVICES, LLC, Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Greg Torrano ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Horizon Actuarial Services, LLC ("Defendant" or "Horizon"), and allege, upon personal knowledge as to his own actions and his counsels' investigations, 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 properly secure and safeguard sensitive Personally Identifiable Information provided by and belonging to its customers, including, without limitation, names, dates of birth, health plan information, and Social Security numbers ("PII").

2. Defendant Horizon provides technical and actuarial consulting services

for benefit plans in the United States.[1] On or around November 12, 2021, Horizon received an email from a group "claiming to have stolen data from its computer servers" on November 10, 2021 and November 11, 2021 (the "Data Breach"). Horizon, after conducting an investigation, paid the group in exchange for an "agreement that they would delete and not distribute or otherwise misuse stolen information." The group provided a list of information they claimed to have stolen from Horizon's servers.

3. On or about January 9, 2022 Horizon determined the information contained the sensitive information of individuals and preliminary list of individuals affected by the Data Breach. Defendant determined that the unauthorized actor accessed and exfiltrated the PII of more than 2,537,261 current and former Horizon customers ("Class Members"), including that of Plaintiff and Class Members.

4. On or around January 13, 2022, Defendant states it began notifying affected Class Members of the Data Breach.

5. Despite learning of the Data Breach in November 2021, Horizon waited to begin informing Class Members until roughly January 13, 2022. Plaintiff did not receive his Notice of Data Incident from Horizon until April 14, 2022 (dated April

[1] Exhibit 1 (Plaintiff Terrano's *Notice of Data Breach* letter)

8, 2022)[2] – more than 5 months after the Data Breach occurred. During this time, Plaintiff and Class Members were unaware that their sensitive personal identifying information had been compromised.

6. Defendant posted a "Notice of Data Incident" on its website (the "Website Notice")[3] detailing the benefit plans for which it provides services. There, it states that Horizon "received information regarding plan participants and their family members for business and compliance purposes." This information included the PII of Plaintiff and Class Members.

7. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to these individuals. Defendant admits that the unencrypted PII accessed and exfiltrated includes highly sensitive information, such as names, dates of birth, health plan information, and Social Security numbers.

8. The exposed PII of Defendant's customers can be sold on the dark web and is in the hands of "the group" of criminals. Plaintiff and Class Members have no ability to protect themselves, as these criminals can easily access and/or offer for sale the unencrypted, unredacted PII to other criminals. Defendant's customers face

[2] Ex 1.
[3] Exhibit 2 ("Website Notice").

a lifetime risk of identity theft, which is heightened by the loss of their Social Security numbers.

9. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of Defendant's customers.

10. Until notified of the breach, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their rest of their lives.

11. Plaintiff bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Defendant's customers; (ii) warn Defendant's customers of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities. Defendant's conduct amounts to negligence and violates federal and state statutes.

12. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address

and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII, and, at the very least, are entitled to nominal damages.

13. Defendant states it this incident and the security of information in its care very seriously.[4] However, Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Defendant's customers' PII was safeguarded, failing to take available steps to prevent an

[4] Exhibit 2 ("Website Notice".)

unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. Plaintiff by this action seeks compensatory damages together with injunctive relief to remediate Horizon's failure to secure Plaintiff's and Class Members' PII, and to provide credit monitoring, identity theft insurance, and credit repair services to protect the Class of Data Breach victims from identity theft and fraud.

II. PARTIES

Plaintiff Greg Torran

15. Plaintiff Greg Torrano is a resident and citizen of the state of California and intends to remain domiciled in and a citizen of the state of California. Plaintiff Torrano lives in Fresno County, California.

16. Plaintiff Torrano received a letter dated April 8, 2022, from Defendant concerning the Data Breach. The letter stated an unauthorized group had stolen data

from Horizon's servers containing his name, date of birth, and Social Security number.[5]

Defendant Horizon Loan Servicing, LLC

17. Defendant Horizon Actuarial Services, LLC is organized under the laws of Delaware and has a principal place of business in Atlanta, Georgia. Horizon's principal place of business is located at 1040 Crown Pointe Parkway, Suite 560, Atlanta, Georgia.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiff will seek leave of Court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

20. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000,

[5] Ex. 1.

exclusive of interest and costs. Moreover, Plaintiffs, numerous other Class Members, and Defendants are citizens of different states.

21. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operated, conducted, engaged in, or carried on a business or business venture in Georgia; had offices in Georgia; committed tortious acts in Georgia; and/or breached a contract in Georgia by failing to perform acts required by the contract to be performed in Georgia. Defendant is organized under the laws of Delaware with its principal place of business and headquarters at 1040 Crown Pointe Parkway, Suite 560, Atlanta, Georgia.

22. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, Defendant conducts substantial business in this district, and Defendant resides in this district. Further, Defendant is headquartered and does business in and/or has offices for the transaction of its customary business in this district.

IV. FACTUAL ALLEGATIONS

Background

23. Horizon Actuarial Services, LLC is a "leading consulting firm that specializes in providing innovative actuarial solutions to multiemployer benefit

plans; [Horizon] proudly serve[s] over 120 pension and health and welfare plans in various industries, including construction, trucking, professional sports, hospitality, entertainment, retail food, and communication."[6] Horizon states that it views its role as "consultants whose responsibility it is to protect the interests of the plan participants by keeping all trustees, both labor and management, well informed and well equipped to navigate the challenges facing their plans."[7]

24. Plaintiff and Class Members are the family of members or members of those benefit plans; as a condition of participating in those benefit plans and receiving services from Defendant, Plaintiff and Class Members were required to entrust some of their most sensitive and confidential information, including, without limitation: name, date of birth, health plan information, and Social Security number. Information that Plaintiff entrusted to Defendant is static, does not change, and can be used to commit myriad financial crimes.

25. In providing services to Plaintiff and Class Members, Defendant generated and retained additional sensitive personal information about Plaintiff and Class Members.

26. Plaintiff and Class Members, as customers of Defendant, relied on

[6] www.horizonactuarial.com/about-us.html (last visited Apr. 27, 2022).
[7] *Id.*

Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

27. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

28. On or around November 10, 2021 and November 11, 2021, an unauthorized group gained unauthorized access to the Horizon servers and exfiltrated data stored there.[8] On November 12, 2021, the group emailed Horizon to inform Horizon of the theft.[9] Horizon determined that the group exfiltrated the PII of more than 2,500,000 individuals.

29. Horizon's website includes the Website Notice. The Website Notice states that Horizon "is providing notice of a data privacy incident on behalf of itself and the benefit plans listed below to whom Horizon Actuarial provides technical and actuarial consulting services (the 'Plans'). Horizon Actuarial received information

[8] Exhibit 3 (sample "Notice of Data Breach" sent to Maine Attorney General's Office).
[9] *Id.*

regarding plan participants and their family members for business and compliance purposes." Those benefit plans include:

a. Airconditioning and Refrigeration Industry Health & Welfare Trust Fund
b. Airconditioning and Refrigeration Industry Retirement Trust Fund
c. Buffalo Laborers Pension Fund
d. Buffalo Laborers Welfare Fund
e. Central Pension Fund of the International Union of Operating Engineers and Participating Employers
f. Fox Valley & Vicinity Labor Pension Plan
g. Fox Valley & Vicinity Labor Welfare Plan
h. IBEW Local 540 Pension Plan
i. IBEW Local 64 Pension Plan
j. Major League Baseball Players Benefit Plan
k. National Hockey League Players Association Health and Benefits Fund
l. National Roofing Industry Pension Plan
m. OCU Health & Welfare Trust
n. OCU Pension Trust
o. Operating Engineers Local 324 Pension Plan
p. Patriot Retirees Voluntary Employees' Beneficiary Association
q. Rocky Mountain UFCW Health Benefit Plan for Retired Employees
r. Rocky Mountain UFCW Retail and Meat Pension Plan
s. Roofers Local 20 Pension Plan
t. Roofers Local No. 20 Health & Welfare Plan
u. Southern Nevada Culinary and Bartenders Pension Fund
v. Teamsters Local 1034 Pension Fund
w. Teamsters Local 27 Pension Fund
x. Teamsters Local 295 Employers Group Welfare Trust
y. Teamsters Local 813 Pension Fund
z. Twin Cities Bakery Drivers Health & Welfare Fund
aa. Twin Cities Bakery Drivers Pension Fund
bb. UA Local 198 Pension Fund
cc. UFCW & Employers Benefit Trust
dd. UFCW Comprehensive Benefit Trust
ee. UFCW Intermountain Health Fund
ff. UFCW Local 711 & Retail Food Employers Benefit Fund

gg. United Union of Roofers Burial Benefit Fund

30. Defendant began reporting the Data Breach to the Attorneys General of various states in March of 2022. On March 9, 2022, Defendant first reported the breach of the PII of 13,198 individual members associated with the Major League Baseball Play Benefit Plan.[10]

31. On March 22, Defendant supplemented its report to the Maine Attorney General three times and provided a Sample Notice to the Attorney General, indicating that another 194,195 individuals were notified of the Data Breach.[11]

32. On April 11, 2022 Defendant provided a Second Supplemental Notice to the Maine Attorney General, indicating 786,012 individuals had been notified.[12]

[10] https://apps.web.maine.gov/online/aeviewer/ME/40/99ac01e4-0ec5-4e69-a27a-f09b00cc3eed.shtml; Defendant later supplemented this report with a second report for this Fund (https://apps.web.maine.gov/online/aeviewer/ME/40/4f268284-cacb-4dc0-b2a5-f5d8811c57da.shtml).

[11] Exhibit 3 (sample "Notice of Data Breach" sent to Maine Attorney General's Office); *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/da4c00e2-64d8-4c54-ab92-d7646fd6c677.shtml (Local 295 IBT Employer Group Pension and Welfare Funds (6,323 members affected); https://apps.web.maine.gov/online/aeviewer/ME/40/a2fd8d06-5eac-41d6-bf68-98ee9d1bd90b.shtml (New York Teamsters Conference Pension and Retirement Fund (42,384 affected)); https://apps.web.maine.gov/online/aeviewer/ME/40/4f268284-cacb-4dc0-b2a5-f5d8811c57da.shtml (Second Notice for Major League Baseball Players Benefit Plan (13,156 affected).

[12] https://apps.web.maine.gov/online/aeviewer/ME/40/b29467de-b33c-4fa4-bb57-9950caa518a4.shtml.

33. On April 15, 2022, Defendant provided a Third Supplemental Notice, indicating 1,309,870 individuals had been notified.[13]

34. On April 18, 2022, Defendant reported that it notified another 224,776 individuals who were associated with the Unite Here Retirement Fund.[14]

35. On or around March 9, 2022 through April of 2022, Defendant sent Plaintiff and Class Members a form "Notice of Data Breach" substantially similar to the sample letters provided to the Maine Attorney General and the Website Notice. The Website Notice Stated, in part:

> **What Happened?**
> On November 12, 2021, Horizon Actuarial received an email from a group claiming to have stolen copies of personal data from its computer servers. Horizon Actuarial immediately initiated efforts to secure its computer servers and with the assistance of third-party computer specialists, launched an investigation into the legitimacy of the claims in the email. Horizon Actuarial also provided notice to law enforcement. During the course of the investigation, Horizon Actuarial negotiated with and paid the group in exchange for an agreement that they would delete and not distribute or otherwise misuse the stolen information.
>
> The investigation revealed that two Horizon Actuarial computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The group

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/9a75003c-3594-4f57-880b-7036f4ee5b8e.shtml
[14] https://apps.web.maine.gov/online/aeviewer/ME/40/1a678bf7-5b5c-4559-98ff-da10838f05e9.shtml.

> provided a list of information they claimed to have stolen. The types of information impacted may include names, dates of birth, Social Security numbers and health plan information.
>
> We provided notice of the incident to the Plans impacted by this event beginning on January 13, 2022 and offered to provide notice on their behalf. Beginning on March 9, 2022, Horizon Actuarial began mailing letters to individuals associated with the Plans that authorized them to do so. These letters include an offer of complimentary fraud and identity theft support services and credit monitoring.
>
> **What We Are Doing.**
>
> Horizon Actuarial takes this incident and the security of information in our care very seriously. We are reviewing our existing security policies and have implemented additional measures to further protect against similar incidents moving forward.

36. Defendant admitted in the sample letter that unauthorized third persons accessed and removed from its network systems sensitive information about customers of Defendant, including, without limitation: "name, date of birth, health plan information, and Social Security number"[15] This sensitive information is static, cannot change, and can be used to commit myriad financial crimes.

37. Plaintiff's and Class Members' unencrypted information may have

[15] Ex. 2.

already been leaked onto the dark web, sold to other cyber criminals, and/or may simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of the affected customers. Unauthorized individuals have unfettered access to the PII of Defendant's customers now that it has been stolen.

38. Defendant did not use reasonable security procedures and practices suitable or adequate to protect the sensitive, unencrypted information it was maintaining for customers, causing the unauthorized exfiltration of the PII of more than 2,500,000 individuals.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII.

39. Defendant acquired, collected, and stored the PII of Defendant's customers.

40. Defendant receives PII from customers and/or their benefit plans as a condition of its services; customers like Plaintiff and Class Members are required to provide and entrust Defendant with highly confidential PII to participate in their respective benefit plans.

41. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known

that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

42. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as customers, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

43. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII. Additionally, Defendant could have destroyed data, including old data that Defendant had no legal right or responsibility to retain.

44. Defendant's negligence in safeguarding Defendant's customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially sensitive financial data.

45. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

46. The Federal Trade Commission ("FTC") defines identity theft as "a

fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[17]

47. The ramifications of Defendant's failure to keep secure Defendant's customers' PII are long lasting and severe. Once Social Security numbers and other PII have been stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

48. The PII of individuals is of high value to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a

[16] 17 C.F.R. § 248.201 (2013).

[17] *Id.*

price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] Criminals also can purchase access to entire sets of information obtained from company data breaches from $900 to $4,500.[20]

49. Social Security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can

[18] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Apr. 27, 2022).

[19] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Apr. 27, 2022).

[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Apr. 27, 2022).

cause a lot of problems.[21]

50. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.

51. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

52. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, in that situation, victims can cancel or

[21] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 27, 2022).

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Apr. 27, 2022).

close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, financial history, and Social Security number.

53. This data commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[23]

54. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

55. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

56. Further, there may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According

[23] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 27, 2022).

to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Defendant's customers' PII, including Social Security numbers and financial account information, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Defendant's customers as a result of such a breach.

58. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damage in addition to any fraudulent use of their PII.

59. Defendant was, or should have been, fully aware of the unique type and

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited Apr. 27, 2022).

the significant volume of data on Defendant's network, comprising millions of individuals' detailed and confidential personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. Although Defendant has offered its customers identity monitoring services for twelve months through Kroll, the offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

61. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Defendant's customers.

Plaintiff Greg Torrano's Experience

62. Plaintiff Torrano receives pension benefits as a retiree and member of the Dallas, Fort Work Local 178 IUOE Union. He receives his pension benefits from the Central Pension Fund of the International Union of Operating Engineers and Participating Employers ("the IUOE Fund") As a condition to receiving services from Horizon, upon information and belief, Plaintiff Torrano's PII was provided by the IUOE Fund to Horizon, which was then entered into Horizon's database and maintained by Defendant.

63. Plaintiff Torrano greatly values his privacy and PII, especially regarding his finances and sensitive information. Prior to the Data Breach, Plaintiff Torrano took reasonable steps to maintain the confidentiality of his PII.

64. Plaintiff Torrano received a letter dated April 8, 2022 from Defendant concerning the Data Breach.[25] The letter stated that unauthorized actors accessed Horizon's network and stole data containing his name, Social Security number, date of birth.

65. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Torrano faces, Defendant offered a one year subscription to a credit monitoring service. However, Plaintiff Torrano has not signed up for the program, as he has an inherent mistrust of the Defendant following the Data Breach.

66. Since learning of the Data Breach, Plaintiff Torrano has spent additional time reviewing his bank statements and credit cards. Since learning of the breach, he has spent approximately two hours every day reviewing his bank, credit and debit card statements.

67. The Data Breach has caused Plaintiff Torrano to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Horizon has not been forthright with information about the Data Breach.

[25] Ex. 1.

68. Plaintiff Torrano plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

69. Additionally, Plaintiff Torrano is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

70. Plaintiff Torrano stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

71. Plaintiff Torrano has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

72. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiff seek to bring this class action on behalf of themselves and a Class (the "Class") defined as follows.

> All individuals in the United States whose PII was accessed or exfiltrated during the Data Breach of Horizon Actuarial Services, LLC, in 2021.

73. Excluded from the Class are the following individuals and/or entities:

Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

74. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

75. Numerosity. Consistent with Fed. R. Civ. P. 23(a)(1), the Class Members are so numerous that their joinder is impracticable. While the exact number of Class Members is unknown, upon information and belief, it is in excess of two and a half million. The number and identities of Class Members can be ascertained through Defendant's records.

76. Commonality. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

b. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

c. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members, respectively, to unauthorized third parties;

d. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

e. Whether and when Defendant learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant committed violations by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices adequate to protect the information compromised in the Data Breach, considering its nature and scope;

i. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual,

consequential, and/or nominal damages as a result of Defendant's wrongful conduct, and if so, in what amount;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct, and if so, in what amount; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

77. Typicality. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance, and their claims arise under the same legal doctrines.

78. Policies Generally Applicable to the Class. As provided under Fed. R. Civ. P. 23(b)(2), Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct in relation to the Class and making final injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff challenge these policies by reference to Defendant's conduct with respect to the Class as a whole.

79. Adequacy of Representation. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff will fairly and adequately represent and protect the interests of the Class Members. No Plaintiff has a disabling conflict of interest with any other Member of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class, and the infringement of rights and the damages they have suffered are typical of other Class Members. Plaintiff also have retained counsel experienced in complex class action litigation, and they intend to prosecute this action vigorously.

80. Superiority and Manageability. Consistent with Fed. R. Civ. P. 23(b)(3), class treatment is superior to all other available methods for the fair and efficient adjudication of this controversy. Among other things, it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Moreover, class action treatment will permit the adjudication of relatively modest claims by Class Members who could not individually afford to litigate a complex claim against a large corporation such as Defendant. Prosecuting the claims pleaded herein as a class action will eliminate the possibility of repetitive litigation. There will be no material difficulty in the management of this action as a class action.

81. Particular issues, such as questions related to Defendant's liability, are

also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the resolution of such common issues would materially advance the resolution of this matter and the parties' interests therein.

82. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. Prosecution of separate actions by Class Members also would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

83. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 82.

84. As a condition of participating in benefit plans or health plans from partners of Defendant, Defendant's customers were obligated to provide and entrust Defendant with certain PII, including their name, birthdate, Social Security number, and health plan information.

85. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

86. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

87. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

88. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure

that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

89. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

90. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

91. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in obtaining services from Defendant.

92. Defendant were subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

93. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of

Defendant's inadequate security practices.

94. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

95. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

96. Plaintiff and the Class had no ability to protect their PII that was in, and remains in, Defendant's possession.

97. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

98. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and

when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

99. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

100. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

101. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

102. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its customers' PII in the face of increased risk of theft.

103. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

104. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to

retain pursuant to regulations.

105. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

106. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

107. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class' PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

108. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

109. Defendant violated Section 5 of the FTC Act by failing to use

reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

110. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

111. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

112. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act 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 Plaintiff and the Class.

113. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost

opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the customers' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

114. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

115. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant

fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

116. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff are now at an increased risk of identity theft or fraud.

117. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

118. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 82.

119. Defendant acquired and maintained the PII of Plaintiff and the Class, including name, birthdate, Social Security number, and health plan information.

120. At the time Defendants acquired the PII and PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the PII and not take unjustified risks when storing the PII.

121. Plaintiff and the Class would not have entrusted their PII to Defendants had they known that Defendants would make the PII internet-accessible, not encrypt

sensitive data elements such as Social Security numbers, and not delete the PII that Defendants no longer had a reasonable need to maintain.

122. Defendant further promised to comply with industry standards and to ensure that Plaintiff's and Class Members' PII would remain protected.

123. Implicit in the agreement between Plaintiff and Class Members and the Defendant

to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

124. In collecting and maintaining the PII of Plaintiff and the Class and publishing the Privacy Policy, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiff and the Class.

125. Plaintiff and the Class fully performed their obligations under the contracts with Defendant.

126. Defendant breached the contracts they made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class, including failing to (i) encrypt or tokenize the sensitive PII of Plaintiff and the Class, (ii) delete such PII that Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

127. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

128. As a direct and proximate result of Defendant's breach of contract, Plaintiff are at an increased risk of identity theft or fraud.

129. As a direct and proximate result of Defendant's breach of contract, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

130. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 82.

131. A relationship existed between Plaintiff and the Class and Defendant in which Plaintiff and the Class put their trust in Defendant to protect the private information of Plaintiff and the Class. Defendant accepted that trust and the concomitant obligations.

132. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

133. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

134. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

135. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and the Class's information in Defendant's possession was adequately secured and protected.

136. Defendant also had a fiduciary duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant, and because

Defendant was the only party in a position to know of its inadequate security measures and capable of taking steps to prevent the Data Breach.

137. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the Class.

138. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

139. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

140. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Class.

141. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themself and all Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiff and Class Members unless

Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personally identifying information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personally identifying information on a cloud-based database;

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

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual

basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

Date: April 28, 2022

Respectfully submitted,

/s/ Gregory J. Bosseler
GREGORY J. BOSSELER
GA Bar #: 742496
MORGAN & MORGAN
191 Peachtree St. NE. STE 4200
Atlanta, GA 30303
Telephone: (404) 496-7318
GBosseler@ForThePeople.com

JOHN A. YANCHUNIS*
KENYA REDDY*

PATRICK BARTHLE*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
jyanchunis@ForThePeople.com
kreddy@ForThePeople.com
pbarthle@ForThePeople.com

Attorneys for Plaintiff and the Proposed Class

** Pro Hac Vice Application Forthcoming*

CERTIFICATE OF SERVICE

I HEREBY CERTIFY on April 28, 2022, a true and correct copy of the foregoing has been furnished via email through the Georgia Court E-Filing Portal to all counsel of record.

/s/ Gregory J. Bosseler
GREGORY J. BOSSELER