Exhibit A

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

GARY ZAHARA, on behalf of himself and all others similarly situated, Plaintiff, v. CBIZ, INC. and PROGRESS SOFTWARE CORPORATION, Defendants.	Case No.: _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Gary Zahara ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Defendant CBIZ, Inc. ("CBIZ") and Defendant Progress Software Corporation ("PSC") (collectively, "Defendants") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated CBIZ clients' employees sensitive information, including their full names, Social Security numbers, 401(k) accounts information, and other sensitive information ("personally identifiable information" or "PII").

2. Defendant CBIZ is a corporation, with "more than 120 offices and 6,500 team members[,]" that provides “financial and benefits and insurance services to organizations of all sizes, as well as individual clients[.]”[1]

3. Defendant PSC advertises itself as an “experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely.”[2]

4. Upon information and belief, former and current employees at CBIZ’s clients are required to entrust Defendants with sensitive, non-public PII, without which Defendants could not perform their regular business activities, in order to obtain employment from CBIZ’s clients. Defendants retain this information for at least many years and even after the relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. On or about May 31, 2023, CBIZ learned that Pension Benefit Information, LLC’s network, which PSC provided software services to and CBIZ relied on for the sending and receiving of sensitive information, had been penetrated by a cyberattack.[3] In response, CBIZ “promptly launched an investigation, with the assistance of cybersecurity professionals, into the nature and scope of the MOVEit Transfer vulnerability."[4] As a result of the investigation, CBIZ concluded–on undisclosed date–that "an unauthorized party exploited the vulnerability and

[1] https://www.cbiz.com/about-us/company-overview (last accessed Sep. 21, 2023).
[2] https://www.progress.com/company (last visited July 19, 2023).
[3] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/d4459dc9-cd5b-4422-921d-b305d5caef7d.shtml (last accessed Sep. 21, 2023).
[4] *Id.*

downloaded files from CBIZ's MOVEit Transfer server, including HBC files containing [Plaintiff's and Class Members'] personal information."[5]

7. According to the untitled letter sent by CBIZ, on behalf of Defendants, to Plaintiff and other victims of the Data Breach (the "Notice Letter"), the compromised PII included individuals' full names, Social Security numbers, and 401(k) account information.[6]

8. Defendants failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect consumers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

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

10. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by their IT vendors to ensure that the PII of

[5] *Id.*
[6] *Id.*

Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an 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 a result, the PII of Plaintiff and Class Members was compromised through disclosure to 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.

11. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Verizon Digital Secure (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in CBIZ's possession and is subject to further unauthorized disclosures so long as CBIZ fails to undertake appropriate and adequate measures to protect the PII so long as CBIZ fails to undertake appropriate and adequate measures to protect the PII.

12. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

II. PARTIES

13. Plaintiff, Gary Zahara, is, and at all times mentioned herein was, an individual and citizen of Naperville, Illinois.

14. Defendant, CBIZ, Inc., is a company incorporated under the state laws of Delaware with its principal place of business located in Independence, Ohio.

15. Defendant, Progress Software Corporation, is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803.

III. JURISDICTION AND VENUE

16. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Massachusetts and have different citizenship from Defendants, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

17. This Court has jurisdiction over Defendants because Defendants operate in this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant PSC's principal place of businesses are located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendants have harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. *Defendants' Businesses*

19. Defendant CBIZ is a corporation, with "more than 120 offices and 6,500 team

members[,]" that provides "financial and benefits and insurance services to organizations of all sizes, as well as individual clients[.]"[7]

20. Defendant PSC advertises itself as an "experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[8]

21. Plaintiff and Class Members are current and former employees at CBIZ's clients.

22. As a condition of obtaining employment at CBIZ's clients, Plaintiff and Class Members were required to entrust Defendants, directly or indirectly, with highly sensitive personal information.

23. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

24. Upon information and belief, Defendants made promises and representations to its clients' employees, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining employment at CBIZ's clients would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

25. Indeed, CBIZ's Privacy Policy provides that: "CBIZ takes reasonable measures to protect CBIZ-Collected PI (excluding public UGC), Client-service PI and Client-service PHI, from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction."[9]

[7] https://www.cbiz.com/about-us/company-overview (last accessed Sep. 21, 2023).
[8] https://www.progress.com/company (last visited July 19, 2023).
[9] https://www.cbiz.com/privacy-policy (last accessed Sep. 21, 2023).

26. Plaintiff and Class Members provided their PII, directly or indirectly, to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

27. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

28. Defendants had duties to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties, and CBIZ had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal duty to keep consumer's PII safe and confidential.

29. Defendants had obligations created by FTC Act, Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

30. Defendants derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. *The Data Breach*

32. On or about October 27, 2023, CBIZ, on behalf of Defendants, began sending Plaintiff and other Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

> On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software, which is used by global organizations, disclosed a vulnerability in their software that had been exploited by an unauthorized third party who was able to download files from MOVEit Transfer. CBIZ and its customers utilize MOVEit Transfer in the regular course of business operations to securely transfer files.
>
> . . .
>
> **What Information Was Involved?** CBIZ's investigation determined that the unauthorized party accessed one or more files relating to current employees or former employees who had a balance in the HBC 401(k) plan as of December 31, 2022, or had any transaction activity (contributions, distributions, loan repayments, etc.) during 2022. These files contained your name, social security number and the account balance of your HBC 401(k) plan as of December 31, 2022.[10]

33. Omitted from the Notice Letter were the dates of the Data Breach, the dates of CBIZ's investigation, any explanation as to why it took CBIZ approximately three months to notify Plaintiff and Class Members of the Data Breach's occurrence after being notified of the cyberattack by PSC, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

34. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without

[10] Notice Letter.

these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

35. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, CBIZ failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

36. The attacker accessed and acquired files from Defendants containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

37. As Plaintiff has already experienced, the PII of Class Members was or will be subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

C. *Defendants Acquire, Collect, And Store Consumers' PII*

38. As a condition to obtain employment at CBIZ's clients, Plaintiff and Class Members were required to give their sensitive and confidential PII, directly or indirectly, to Defendants.

39. CBIZ retains and stores this information with PSC and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendants would be unable to perform their services.

40. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

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

42. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by CBIZ exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

43. Upon information and belief, Defendants made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

44. Indeed, CBIZ's Privacy Policy provides that: "CBIZ takes reasonable measures to protect CBIZ-Collected PI (excluding public UGC), Client-service PI and Client-service PHI, from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction."[11]

45. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

E. *Defendants Knew or Should Have Known of the Risk Because Financial Companies and Software Companies In Possession Of PII Are Particularly Suspectable To Cyber Attacks*

46. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

[11] https://www.cbiz.com/privacy-policy (last accessed Sep. 21, 2023).

47. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting financial companies and software companies that collect and store PII, like Defendants, preceding the date of the breach.

48. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[12]

49. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

50. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

51. As custodians of PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable

[12] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

[13] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

consequences if their data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

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

53. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

54. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' servers, amounting to more than thirty thousand individuals' detailed PII,[14] and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

55. Additionally, as companies became more dependent on computer systems to run their business,[15] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[16]

---

[14] According to the breach report submitted to the Office of the Maine Attorney General, 35,845 persons were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/d4459dc9-cd5b-4422-921d-b305d5caef7d.shtml (last accessed Sep. 21, 2023).

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

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

56. In the Notice Letter, on behalf of CBIZ offers to cover 24 months of identity monitoring for Plaintiff and Class Members. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

57. CBIZ's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendants' computer systems.

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

59. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

60. As a financial company and software company in possession of CBIZ's clients' employees' PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if their data security systems, or those on which it transferred PII, were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

F. *Value Of Personally Identifiable Information*

61. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[17] 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."[18]

62. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[19]

63. For example, PII can be sold at a price ranging from $40 to $200.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

64. Social Security numbers are among the worst kind of PII 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

[17] 17 C.F.R. § 248.201 (2013).
[18] *Id.*
[19] *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 Oct. 17, 2022).
[20] *Here's How Much Your PII 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 Oct. 17, 2022).
[21] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

experienced by Plaintiff and some Class Members, 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 cause a lot of problems.[22]

65. What's 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 the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

66. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he 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."

67. 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, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names and Social Security numbers.

[22] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

68. This data demands 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 . . . [is] worth more than 10x on the black market."[23]

69. 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.

70. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According 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]

G. *Defendants Failed to Comply with FTC Guidelines*

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in

---

[23] Tim 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 Oct. 17, 2022).

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

72. In October 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

73. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. These FTC enforcement actions include actions against financial companies and software companies, like Defendants.

76. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and CBIZ failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

77. Defendants were at all times fully aware of their obligations to protect the PII of the consumers in their networks yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

H. *CBIZ Failed to Comply with the Gramm-Leach-Bliley Act*

78. CBIZ is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

79. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

80. CBIZ collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period CBIZ was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

81. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial

Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

82. Accordingly, CBIZ's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

83. Both the Privacy Rule and Regulation P require financial institutions to provide consumers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, CBIZ violated the Privacy Rule and Regulation P.

84. Upon information and belief, CBIZ failed to provide annual privacy notices to consumers after the relationship ended, despite retaining these consumers' PII and storing that PII on CBIZ's network systems.

85. CBIZ failed to adequately inform their consumers that they were storing and/or sharing, or would store and/or share, the consumers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the consumer relationship ended.

86. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

87. As alleged herein, CBIZ violated the Safeguard Rule.

88. CBIZ failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of consumer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

89. CBIZ violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and

Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

I. *Defendants Failed to Comply with Industry Standards*

90. As noted above, experts studying cybersecurity routinely identify financial companies and software companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

91. Some industry best practices that should be implemented by financial companies and software companies dealing with sensitive PII, like Defendants, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

92. Other best cybersecurity practices that are CBIZ in the financial services and software industries include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

93. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

94. Defendants failed to comply with these accepted standards in the financial esrvices and software industries, thereby permitting the Data Breach to occur.

J. *Defendants Breached Their Duties to Safeguard Plaintiff's and the Class's PII*

95. In addition to their obligations under federal and state laws, Defendants owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII of Class Members

96. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard their computer systems and data and failed to audit, monitor, or ensure the integrity of their vendor's data security practices. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect CBIZ's clients' employees' PII;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;

e. Failing to sufficiently train their employees and vendors regarding the proper handling of CBIZ's clients' employees' PII;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to the Gramm-Leach-Bliley Act and industry standards for cybersecurity as discussed above; and,

h. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

97. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access their computer networks and systems which contained unsecured and unencrypted PII.

98. Had Defendants remedied the deficiencies in their information storage and security systems or those of their vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

K. ***Common Injuries & Damages***

99. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss

of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in CBIZ's possession and is subject to further unauthorized disclosures so long as CBIZ fails to undertake appropriate and adequate measures to protect the PII.

L. ***The Data Breach Increases Victims' Risk Of Identity Theft***

100. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

101. As Plaintiff has already experienced, the unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

102. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

103. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

104. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

105. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[25]

106. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

107. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

[25] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than CBIZ credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

108. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

109. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

110. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

M. ***Loss Of Time To Mitigate Risk Of Identity Theft And Fraud***

111. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

112. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must take measures to protect themselves.

113. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon

receiving the Notice Letter, changing passwords and resecuring their own computer networks, replacing credit and/or debit cards impacted by the Data Breach, and contacting financial institutions to sort out fraudulent activity on their accounts and otherwise ensure their accounts are secure.

114. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

115. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

116. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

---

[26] *See* United States Government Accountability Office, GAO-07-737, PII: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[27] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[28] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

N. *Diminution Value Of PII*

117. PII is a valuable property right.[29] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

118. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[30]

119. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[31,32]

120. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[33]

121. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[34]

122. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by

---

[29] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[30] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[31] https://datacoup.com/
[32] https://digi.me/what-is-digime/
[33] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[34] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

123. 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, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names and Social Security numbers.

124. 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.

125. The fraudulent activity resulting from the Data Breach may not come to light for years.

126. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

127. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to more than thirty thousand individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

O. ***Future Cost of Credit & Identity Theft Monitoring is Reasonable and Necessary***

129. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, the volume of data obtained in the Data Breach, and Plaintiff's reports that his PII has already been disseminated on the dark web (as discussed below), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

130. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

131. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

132. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

P. ***Loss Of The Benefit Of The Bargain***

133. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to accept employment at CBIZ's clients, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for, or being paid less for, the necessary data security to protect the PII, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with CBIZ's clients.

Q. ***Plaintiff's Experience***

134. Plaintiff Gary Zahara is a current employee at Hudson's Bay Company, which contracted with CBIZ for services.[35]

135. In order to obtain employment at Hudson's Bay Company, Plaintiff was required to provide his PII, directly or indirectly, to Defendants, including his name, Social Security number, and other sensitive information.

136. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their systems.

137. Plaintiff Zahara is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies.

138. Plaintiff Zahara received the Notice Letter, by U.S. mail, from CBIZ, dated October 27, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and

[35] The Notice Letter.

obtained by unauthorized third parties, including his name, Social Security number, and the account balance of his HBC 401(k) plan as of December 31, 2022.

139. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring his own computer network, replacing credit and/or debit cards impacted by the Data Breach, and contacting financial institutions to sort out fraudulent activity on his accounts and to otherwise ensure his accounts are secure. Plaintiff has spent significant time on reasonable efforts to mitigate the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

140. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in CBIZ's possession and is subject to further unauthorized disclosures so long as CBIZ fails to undertake appropriate and adequate measures to protect the PII.

141. Plaintiff additionally suffered actual injury in the form of his PII being disseminated on the dark web, according to Verizon Digital Secure, which, upon information and belief, was caused by the Data Breach.

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

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

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

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

146. Plaintiff Zahara has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

147. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

148. Specifically, Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States whose PII was impacted as a result of the Data Breach (the "Class").

Illinois Subclass
All individuals in the state of Illinois whose PII was impacted as a result of the Data Breach (the "Illinois Subclass").

149. Excluded from the Classes are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

150. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class and/or Illinois Subclass, as well as add subclasses, before the Court determines whether certification is appropriate.

151. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

152. Numerosity: The Class Members are so numerous that joinder of all members is impracticable. Although the exact number of Class Members is currently unknown to Plaintiff and exclusively in the possession of Defendants, according to the breach report submitted to the Office of the Maine Attorney General, approximately 35,000 persons were impacted in the Data Breach.[36] The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by PBI sending them Notice Letters).

153. Commonality: There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

[36]https://apps.web.maine.gov/online/aeviewer/ME/40/d4459dc9-cd5b-4422-921d-b305d5caef7d.shtml (last accessed Sep. 21, 2023).

b. Whether Defendants' conduct violated the FTCA and/or GBLA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class Members' PII;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed duties to Class Members to safeguard their PII;

j. Whether Defendants breached their duty to Class Members to safeguard their PII;

k. Whether hackers obtained Class Members' PII via the Data Breach;

l. Whether Defendants had legal duties to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Defendants breached their duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

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

154. Typicality: Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

156. Predominance: Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over

any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

157. Superiority: A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

158. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

159. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice Letters by PBI.

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

160. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

161. CBIZ requires its clients' employees, including Plaintiff and Class Members, to submit non-public PII to Defendants in the ordinary course of providing its services.

162. Defendants gathered and stored the PII of Plaintiff and Class Members as part of their businesses of soliciting their services to their clients, which solicitations and services affect commerce.

163. Plaintiff and Class Members entrusted Defendants with their PII with the understanding that Defendants would safeguard their information.

164. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

165. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants owed duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. CBIZ's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

166. Defendants had duties to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

167. CBIZ's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

168. Defendants owed duties of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

169. Defendants' duties of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential PII, a necessary part of being employees at CBIZ's clients.

170. Defendants' duties to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

171. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

172. Defendants also had duties to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

173. Moreover, Defendants had duties to promptly and adequately notify Plaintiff and the Class of the Data Breach.

174. Defendants had and continues to have duties to adequately disclose that the PII of Plaintiff and the Class within Defendants' possession might have been 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.

175. Defendants breached their duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

176. Defendants violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

177. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

178. Defendants' violation of Section 5 of the FTC Act and GLBA constitutes negligence.

179. 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.

180. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

181. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services and software industries.

182. Defendants have 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.

183. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

184. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

185. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

186. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

187. Defendants' duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

188. CBIZ has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

190. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent

harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

191. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Verizon Digital Secure (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in CBIZ's possession and is subject to further unauthorized disclosures so long as CBIZ fails to undertake appropriate and adequate measures to protect the PII so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

192. As a direct and proximate result of Defendants' negligence, 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.

193. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long

as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

194. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

195. Defendants' negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

196. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class against Defendant CBIZ)

197. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this count against Defendant CBIZ ("Defendant" for the purposes of this count).

198. Defendant entered into written contracts with its clients, including Hudson's Bay Company, to provide financial, administrative, and/or other services.

199. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

200. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered

into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, the clients' employees—Plaintiffs and Class Members—would be harmed.

201. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' PII from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

202. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

203. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

204. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

205. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for or had payments made on their behalf for services from CBIZ and/or its agents and/or provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received from CBIZ the services that were the subject of the transaction and should have had their PII protected with adequate data security.

206. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to them.

Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

207. Defendants failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

208. Defendants acquired the PII through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

209. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendants or obtained employment at CBIZ's clients.

210. Plaintiff and Class Members have no adequate remedy at law.

211. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

212. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Verizon Digital Secure (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in CBIZ's possession

and is subject to further unauthorized disclosures so long as CBIZ fails to undertake appropriate and adequate measures to protect the PII so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

213. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

214. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
Violation Of The Illinois Consumer Fraud Act
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiff and the Illinois Subclass)

215. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein, and brings this claim on behalf of himself and the Illinois Subclass (the "Class" for the purposes of this count).

216. Plaintiff and the Class are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e).

217. Plaintiff, the Class, and Defendants are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

218. Defendants are engaged in "trade" or "commerce," including the provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

219. Defendants engage in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

220. Defendants' acts, practices, and omissions were done in the course of Defendants' businesses of marketing, offering for sale, and selling their services in the State of Illinois.

221. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including, but not limited to, the following:

a. failure to maintain adequate computer systems and data security practices to safeguard current and former employees' PII;

b. failure to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the personal information it was collecting and maintaining from theft;

c. failure to disclose in a timely and accurate manner to Plaintiff and the Class Members the material fact of Defendants' data breach;

d. misrepresenting material facts to Plaintiff and the Class, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft;

e. misrepresenting material facts to the class, in connection with the sale of goods and services, by representing that Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class members' PII, and

f. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class members' PII from further unauthorized disclosure, release, data breaches, and theft.

222. In addition, Defendants' failure to disclose that their computer systems were not well protected and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Class; and (b) defeat Plaintiff's and Class members' ordinary, foreseeable and reasonable expectations concerning the security of their PII on Defendants' servers.

223. Defendants intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Defendants' offering of goods and services and storing Plaintiff's and Class members' PII on its servers, in violation of the Illinois CFA.

224. Defendants also engaged in unfair acts and practices by failing to maintain the privacy and security of class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach.

225. These unfair acts and practices violated duties imposed by laws including Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), Gramm-Leach-Bliley Act, and similar state laws.

226. Defendants' wrongful practices occurred in the course of trade or commerce.

227. Defendants' wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendants that

applied to all Class members and were repeated continuously before and after Defendants obtained PII from Plaintiff and Class members.

228. All Class members have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

229. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered harm, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Verizon Digital Secure (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in CBIZ's possession and is subject to further unauthorized disclosures so long as CBIZ fails to undertake appropriate and adequate measures to protect the PII so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

230. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff seeks actual, compensatory, and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the Illinois CFA.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class and Illinois Subclass, pursuant to Federal Rule of Civil Procedure 23;

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

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

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants 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 Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants 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 Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendants 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;

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

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

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their

confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect himself;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvi. 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 Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: November 10, 2023

Respectfully submitted,

/s/ Randi Kassan

Randi Kassan
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

Counsel for Plaintiff and the Proposed Class