UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

MARK S. HOLDEN, RICHARD ANDISIO, EDWARD MARSHALL, ANN MARIE MARSHALL, ARTHUR CHRISTIANI, JOHNIELLE DWYER, PAWEL KRZYKOWSKI, MARIOLA KRZYNOWEK, JAMES HOWE, and CINDY A. PEREIRA, individually, and on behalf of all others similarly situated, Plaintiffs, v. GUARDIAN ANALYTICS, INC., ACTIMIZE INC., and WEBSTER BANK, N.A., Defendants.	Case No. 23-2115 CLASS ACTION JURY TRIAL DEMANDED

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Mark S. Holden, Richard Andisio, Edward Marshall, Ann Marie Marshall, Arthur Christiani, Johnielle Dwyer, Pawel Krzykowski, Mariola Krzynowek, James Howe, and Cindy A. Pereira (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Consolidated Amended Class Action Complaint against Guardian Analytics, Inc. ("Guardian"), Actimize Inc. ("Actimize"), and Webster Bank, N.A. ("Webster Bank") (collectively, "Defendants") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard their and at least 191,563 other individuals' personally identifiable

information ("PII"), including names, Social Security numbers, and financial account numbers.

2. Guardian, which was acquired by Actimize in 2020, provides fraud detection services to Webster Bank. Actimize is a company that is owned by NICE Ltd.

3. Between November 27, 2022 and January 26, 2023, unauthorized individuals had access to Guardian's network systems and acquired the PII of Plaintiffs and Class members (the "Data Breach").

4. Defendants owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their PII from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII was exposed as a result of the Data Breach.

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, violations of the Connecticut Unfair Trade Practices Act, and declaratory judgment and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Mark S. Holden

7. Plaintiff Mark S. Holden is a citizen of the State of Connecticut.

8. Plaintiff Holden was required to provide his PII to Webster Bank in connection with using banking services from Webster Bank.

9. Based on representations made by Webster Bank, Plaintiff Holden believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Holden provided his PII to Webster Bank in connection with or in exchange for banking services.

10. In connection with services provided to Plaintiff Holden, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

11. Had Plaintiff Holden known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

12. Plaintiff Holden received letters from Webster Bank, including one notifying him that his PII was exposed in the Data Breach and two notifying him that his businesses' information was exposed in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff Holden has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Plaintiff Richard Andisio

14. Plaintiff Richard Andisio is a citizen of the State of Connecticut.

15. Plaintiff Andisio was required to provide his PII to Webster Bank in connection with using banking services from Webster Bank.

16. Based on representations made by Webster Bank, Plaintiff Andisio believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Andisio provided his PII to Webster Bank in connection with or in exchange for banking services.

17. In connection with services provided to Plaintiff Andisio, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

18. Had Plaintiff Andisio known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

19. Plaintiff Andisio received a letter from Webster Bank notifying him that his PII was exposed in the Data Breach.

20. As a direct result of the Data Breach, Plaintiff Andisio has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Plaintiff Edward Marshall

21. Plaintiff Edward Marshall is a citizen of the State of Connecticut.

22. Plaintiff Marshall was required to provide his PII to Webster Bank in

connection with using banking services from Webster Bank.

23. Based on representations made by Webster Bank, Plaintiff Marshall believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Marshall provided his PII to Webster Bank in connection with or in exchange for banking services.

24. In connection with services provided to Plaintiff Marshall, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

25. Had Plaintiff Marshall known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

26. Plaintiff Marshall received a letter from Webster Bank notifying him that his PII was exposed in the Data Breach.

27. Plaintiff Marshall spent time signing up for credit monitoring offered to victims of the Data Breach by Webster Bank and has spent time reviewing reports provided by that service.

28. As a direct result of the Data Breach, Plaintiff Marshall has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Plaintiff Ann Marie Marshall

29. Plaintiff Ann Marie Marshall is a citizen of the State of Connecticut.

30. Plaintiff Marshall was required to provide her PII to Webster Bank in connection with using banking services from Webster Bank.

31. Based on representations made by Webster Bank, Plaintiff Marshall believed that Webster Bank had implemented and maintained reasonable security and practices to protect her PII. With this belief in mind, Plaintiff Marshall provided her PII to Webster Bank in connection with or in exchange for banking services.

32. In connection with services provided to Plaintiff Marshall, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

33. Had Plaintiff Marshall known that Defendants do not adequately protect the PII in their possession, she would not have agreed to provide Webster Bank with her PII.

34. Plaintiff Marshall received a letter from Webster Bank notifying her that her PII was exposed in the Data Breach.

35. Plaintiff Marshall spent time signing up for credit monitoring offered to victims of the Data Breach by Webster Bank and has spent time reviewing her financial accounts and reports provided by that service.

36. As a direct result of the Data Breach, Plaintiff Marshall has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII; deprivation of the value of her PII; and overpayment for services that did not include adequate data security.

Plaintiff Arthur Christiani

37. Plaintiff Arthur Christiani is a citizen of the State of Connecticut.

38. Plaintiff Christiani was required to provide his PII to Webster Bank in connection with using banking services from Webster Bank.

39. Based on representations made by Webster Bank, Plaintiff Christiani believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Christiani provided his PII to Webster Bank in connection with or in exchange for banking services.

40. In connection with services provided to Plaintiff Christiani, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

41. Had Plaintiff Christiani known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

42. Plaintiff Christiani received a letter from Webster Bank notifying him that his PII was exposed in the Data Breach.

43. As a result of the Data Breach, Plaintiff Christiani's Venmo account was hacked and fraudulent activity appeared in his account.

44. Plaintiff Christiani spent approximately 2 hours dealing with the Data Breach, including researching the Data Breach and monitoring his financial accounts and credit report.

45. As a direct result of the Data Breach, Plaintiff Christiani has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity

theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Plaintiff Johnielle Dwyer

46. Plaintiff Johnielle Dwyer is a citizen of the State of Connecticut.

47. Plaintiff Dwyer was required to provide her PII to Webster Bank in connection with using banking services from Webster Bank.

48. Based on representations made by Webster Bank, Plaintiff Dwyer believed that Webster Bank had implemented and maintained reasonable security and practices to protect her PII. With this belief in mind, Plaintiff Dwyer provided her PII to Webster Bank in connection with or in exchange for banking services.

49. In connection with services provided to Plaintiff Dwyer, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

50. Had Plaintiff Dwyer known that Defendants do not adequately protect the PII in their possession, she would not have agreed to provide Webster Bank with her PII.

51. Plaintiff Dwyer received a letter from Webster Bank notifying her that her PII was exposed in the Data Breach.

52. Plaintiff Dwyer spent time dealing with the Data Breach, including spending time researching the Data Breach and monitoring her financial accounts.

53. As a direct result of the Data Breach, Plaintiff Dwyer has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII; deprivation of

the value of her PII; and overpayment for services that did not include adequate data security.

Plaintiff Pawel Krzykowski

54. Plaintiff Pawel Krzykowski is a citizen of the State of Connecticut.

55. Plaintiff Krzykowski was required to provide his PII to Webster Bank in connection with using banking services from Webster Bank.

56. Based on representations made by Webster Bank, Plaintiff Krzykowski believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Krzykowski provided his PII to Webster Bank in connection with or in exchange for banking services.

57. In connection with services provided to Plaintiff Krzykowski, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

58. Had Plaintiff Krzykowski known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

59. Plaintiff Krzykowski received a letter from Webster Bank notifying him that his PII was exposed in the Data Breach.

60. Plaintiff Krzykowski has spent time dealing with the Data Breach, including reviewing his financial accounts and dealing with an increased number of spam calls, texts, and emails caused by the Data Breach.

61. As a direct result of the Data Breach, Plaintiff Krzykowski has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity

theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Plaintiff Mariola Krzynowek

62. Plaintiff Mariola Krzynowek is a citizen of the State of Connecticut.

63. Plaintiff Krzynowek was required to provide her PII to Webster Bank in connection with using banking services from Webster Bank.

64. Based on representations made by Webster Bank, Plaintiff Krzynowek believed that Webster Bank had implemented and maintained reasonable security and practices to protect her PII. With this belief in mind, Plaintiff Krzynowek provided her PII to Webster Bank in connection with or in exchange for banking services.

65. In connection with services provided to Plaintiff Krzynowek, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

66. Had Plaintiff Krzynowek known that Defendants do not adequately protect the PII in their possession, she would not have agreed to provide Webster Bank with her PII.

67. Plaintiff Krzynowek received a letter from Webster Bank notifying her that her PII was exposed in the Data Breach.

68. Plaintiff Krzynowek has spent time dealing with the Data Breach, including reviewing his financial accounts and dealing with an increased number of spam calls, texts, and emails caused by the Data Breach.

69. As a direct result of the Data Breach, Plaintiff Dwyer has suffered injury

and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII; deprivation of the value of her PII; and overpayment for services that did not include adequate data security.

Plaintiff James Howe

70. Plaintiff James Howe is a citizen of the State of Connecticut.

71. Plaintiff Howe was required to provide his PII to Webster Bank in connection with using banking services from Webster Bank.

72. Based on representations made by Webster Bank, Plaintiff Howe believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Howe provided his PII to Webster Bank in connection with or in exchange for banking services.

73. In connection with services provided to Plaintiff Howe, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

74. Had Plaintiff Howe known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

75. Plaintiff Howe received a letter from Webster Bank notifying him that his PII was exposed in the Data Breach.

76. Plaintiff Howe has spent time dealing with the Data Breach, including reviewing his financial accounts and dealing with an increased number of spam calls, texts, and emails caused by the Data Breach.

77. Additionally, in December 2022, Plaintiff Howe experienced an

unauthorized withdrawal from his account at Webster Bank. Plaintiff has spent significant time addressing the ramifications of this fraud, including closing his account with Webster Bank and transferring his funds to a different bank.

78. As a direct result of the Data Breach, Plaintiff Howe has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Plaintiff Cindy A. Pereira

79. Plaintiff Cindy A. Pereira is a citizen of the State of Connecticut.

80. Plaintiff Pereira was required to provide her PII to Webster Bank in connection with using banking services from Webster Bank.

81. Based on representations made by Webster Bank, Plaintiff Pereira believed that Webster Bank had implemented and maintained reasonable security and practices to protect her PII. With this belief in mind, Plaintiff Pereira provided her PII to Webster Bank in connection with or in exchange for banking services.

82. In connection with services provided to Plaintiff Pereira, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

83. Had Plaintiff Pereira known that Defendants do not adequately protect the PII in their possession, she would not have agreed to provide Webster Bank with her PII.

84. Plaintiff Pereira received a letter from Webster Bank notifying her that her PII was exposed in the Data Breach.

85. Plaintiff Pereira has spent time dealing with the Data Breach, including reviewing her financial accounts and dealing with an increased number of spam calls, texts, and emails caused by the Data Breach.

86. Plaintiff Pereira has spent time dealing with the Data Breach, including increased monitoring of her financial accounts, researching the Data Breach, and signing up for credit monitoring provided to victims by Webster Bank.

87. As a direct result of the Data Breach, Plaintiff Pereira has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII; deprivation of the value of her PII; and overpayment for services that did not include adequate data security.

Defendants

88. Defendant Guardian Analytics, Inc. is a corporation that was formed under the laws of Delaware. Guardian Analytics' principal place of business is located at 221 River St., Hoboken, NJ 07030. Defendant Guardian Analytics can be served via its Registered Agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

89. Defendant Actimize Inc. is a corporation that was formed under the laws of Delaware. Actimize's principal place of business is located at 221 River St., Hoboken, NJ 07030. Defendant Actimize can be served via its Registered Agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

90. Defendant Webster Bank, N.A. is a national bank that has its principal place of business in Connecticut. Webster Bank is headquartered at 200 Elm St.,

Stamford, CT 06902. Webster Bank can be served at its principal place of business.

JURISDICTION AND VENUE

91. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

92. This Court has personal jurisdiction over Defendants Guardian and Actimize because Guardian and Actimize have their principal place of business in New Jersey. The Court has personal jurisdiction over Defendant Webster Bank because Webster Bank contracts with Guardian, a company headquartered in New Jersey, and therefore purposely availed itself to the laws of New Jersey.

93. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Defendants Guardian and Actimize have their principal place of business in Hudson County, New Jersey, and a substantial part of the events giving rise to Plaintiffs' claims arose in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

94. Guardian is a company that provides "behavioral analytics and machine learning solutions for preventing banking fraud and anti-money laundering."[1] Guardian was acquired by Actimize, which claims to be the "largest and broadest provider of

[1] *About Guardian Analytics*, GUARDIAN ANALYTICS, https://guardiananalytics.com/about-guardian-analytics/ (last accessed Apr. 14, 2023).

financial crime, risk and compliance solutions for regional and global financial institutions."[2]

95. Webster Bank is a "commercial bank that delivers financial solutions to businesses, individuals, families and partners."[3] The company claims to control over $70 billion in assets.[4]

96. Guardian provides Webster Bank with "fraud detection services."[5] Webster Bank provided Guardian with its customers' PII in exchange for these services.

97. In the regular course of their business, Defendants collect and maintain the PII of their clients and their clients' customers.

98. Guardian's website contains a privacy policy regarding the data it collects through its website which states: "The privacy and protection of your personal information is important to us. We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it."[6]

99. Actimize's website contains a privacy policy regarding the data it collects through its website which states, "Your privacy is important to us," and goes on to state,

---

[2] *Id.*

[3] *About*, WEBSTER BANK, https://www.websterbank.com/about/ (last accessed Aug. 24, 2023).

[4] *Id.*

[5] *See Notice of Data Breach*, WEBSTER BANK, https://apps.web.maine.gov/online/aeviewer/ME/40/a42f73e8-720b-41a2-b892-18181e799668/25a99f73-65d3-4c27-bea6-9440850e90c7/document.html (last accessed Aug. 24, 2023).

[6] *Privacy Policy*, GUARDIAN ANALYTICS, https://guardianananalytics.com/privacy-policy/ (last accessed Apr. 14, 2023).

"[Actimize] implements data security systems and procedures to secure the information stored on [Actimize] computer servers."[7]

100. Webster Bank has a page on its website dedicated to customer privacy. The page states, among other representations, "We take the privacy and security of your information seriously and our number one goal is to give you peace of mind when it comes to your protection."[8]

101. Plaintiffs and Class members are or were customers of a Webster Bank and entrusted Defendants with their PII.

The Data Breach

102. Between November 27, 2022 and January 22, 2023, unauthorized individuals had access to Guardian's network systems.[9] Those unauthorized individuals acquired the PII of Plaintiffs and Class members and posted the information on the internet.[10] This has left all of the Plaintiffs and Class members at an imminent risk of fraud and identity theft, if they have not already experienced them.

103. Guardian notified Webster Bank of the Data Breach on January 26, 2023.[11] However, Webster Bank did not begin reporting the Data Breach to Plaintiffs, Class members, and state authorities until on or about April 10, 2023. Thus, Plaintiffs' and

---

[7] *NICE Privacy Notice*, ACTIMIZE, https://www.nice.com/company/legal/privacy-policy (last accessed Aug. 24, 2023).

[8] *Safety and Security*, Webster Bank, https://www.websterbank.com/security/ (last accessed Aug. 24, 2023).

[9] *See Notice of Data Breach*, n.5, *supra*.

[10] *Id.*

[11] *Id.*

Class members' PII was in the hands of cybercriminals for over two months before they were warned that the Data Breach affected this information.

104. The notice that Webster Bank sent to those affected by the Data Breach states the information that was disclosed included a person's "name, Social Security number, and financial account number."[12]

Defendants Knew that Criminals Target PII

105. At all relevant times, Defendants knew, or should have known, that the PII that they collected was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

106. It is well known among companies that store sensitive personally identifying information that such information—such as the Social Security numbers ("SSNs") and financial information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers …. Many of them were caused by flaws in … systems either online or in stores."[13]

[12] *Id.*

[13] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

107. PII is a valuable property right.[14] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[15] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[16] PII is so valuable to identity thieves that once it has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

108. Identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches including the information exposed in the Data Breach can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

109. Consumers place a high value on the privacy of their data, as they should. Indeed, studies confirm that "when privacy information is made more salient and

---

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[15] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[16] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

110. Given these facts, any company that transacts business with a consumer and then compromises the privacy of the consumer's PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

111. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[18] [19]

112. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without

[17] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[18] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Aug. 24, 2023).

[19] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). 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." 12 C.F.R. § 1022.3(g).

permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[20]

113. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[21]

114. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim.

115. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. *TIME* quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[22]

---

[20] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[21] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Aug. 24, 2023).

[22] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

116. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a victim discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some victims up to three years to learn that information.[23]

117. Plaintiffs and Class members must now live with the knowledge that their PII is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiffs and the Other Class members

118. Plaintiffs and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risk which justifies or necessitates expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ACTION ALLEGATIONS

119. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

---

[23] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

120. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All persons whose personally identifiable information was accessed in the Data Breach by unauthorized persons, including all who were sent a notice of the Data Breach.

121. Excluded from the Class are Guardian Analytics, Inc., Actimize Inc., Webster Bank, N.A., and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

122. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

123. The members of the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Webster Bank reported to the Maine Attorney General that approximately 191,563 of its customers' information was exposed in the Data Breach.[24]

124. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

[24] *Data Breach Notifications*, OFF. OF THE MAINE ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/a42f73e8-720b-41a2-b892-18181e799668.shtml (last accessed Aug. 24, 2023).

b. whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;

c. whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

d. whether Defendants breached their duties to protect Plaintiffs' and Class members' PII; and

e. whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

125. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison in both quantity and quality to the numerous common questions that dominate this action.

126. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

127. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to or that conflict with the Class they seek to represent. Plaintiffs

have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

128. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

129. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

130. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting the PII in Defendants' possession, custody, or control.

131. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and Class members' PII and the importance of maintaining secure

systems. Defendants knew or should have known that they faced an increased threat of customer data theft, as judged by the many recent data breaches by individuals targeting companies that stored PII.

132. Given the nature of Defendants' business, the sensitivity and value of the PII they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

133. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class members' PII by failing to or contracting with companies that failed to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class members' PII.

134. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to or contracting with companies that failed to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

135. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

136. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

137. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

138. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair … practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

139. Defendants' violation of Section 5 of the FTCA constitutes negligence per se.

140. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

141. The harm occurring as a result of the Data Breach is the type of harm

Section 5 of the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class members as a result of the Data Breach.

142. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

143. The injury and harm that Plaintiffs and Class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA. Plaintiffs and Class members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT
(Against Defendant Webster Bank)

144. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

145. Plaintiffs bring this claim only against Webster Bank.

146. In connection with the dealings Plaintiffs and Class members had with Defendants, Plaintiffs and Class members entered into implied contracts with Webster Bank.

147. Pursuant to these implied contracts, Plaintiffs and Class members provided Webster Bank with their PII, directly or indirectly, in order for Webster Bank to provide services. In exchange, Webster Bank agreed to, among other things, and Plaintiffs and Class members understood that Webster Bank would: (1) provide services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

148. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Webster Bank, on the other hand. Indeed, Webster Bank was clear in its representations regarding privacy, and on the basis of those representations, Plaintiffs understood that Webster Bank supposedly respects and is committed to protecting customer privacy.

149. Had Plaintiffs and Class members known that Webster Bank would not adequately protect its customers' and former customers' PII, they would not have provided Webster Bank with their PII.

150. Plaintiffs and Class members performed their obligations under the implied contracts when they provided Webster Bank with their PII, either directly or indirectly.

151. Webster Bank breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

152. Webster Bank's breach of its obligations of the implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

153. Plaintiffs and all other Class members were damaged by Webster Bank's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased and imminent risk of identity theft—a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII was breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) they lost time and money

incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT IV
BREACH OF FIDUCIARY DUTY
(against Defendant Webster Bank)

154. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

155. Plaintiffs and Class members gave Webster Bank their PII in confidence believing that Webster Bank would protect that information. Plaintiffs and Class members would not have provided Webster Bank with this information had they known it would not be adequately protected.

156. Webster Bank's acceptance and storage of Plaintiffs' and Class members' PII created a fiduciary relationship between Webster Bank and Plaintiffs and Class members. In light of this relationship, Webster Bank must act in good faith primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiffs' and Class Members' PII.

157. Due to the nature of the relationship between Webster Bank and Plaintiffs and Class members, Plaintiffs and Class members were entirely reliant upon Webster Bank to ensure that their PII was adequately protected. Plaintiff and Class members had no way of verifying or influencing the nature and extent of Webster Bank's data security policies and practices, and Webster Bank was in an exclusive position to guard against the Data Breach.

158. Webster Bank has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that

duty by, among other things, failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII, failing to safeguard Plaintiffs' and Class members' PII it collected, failing to ensure Plaintiffs' and Class members' PII was shared with entities with adequate and proper data protection systems in place, and failing to notify Plaintiffs and Class members of the Data Breach in a timely manner.

159. As a direct and proximate result of Webster Bank's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise and theft of their PII; (iii) out-of-pocket expenses associated with the prevention and detection of and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Webster Bank's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

160. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

161. This claim is pleaded in the alternative to the breach of implied contract claim.

162. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of monies paid for services to Webster Bank, who then used these funds to pay Guardian and Actimize.

163. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class members. Defendants also benefitted from the receipt of Plaintiffs' and Class members' PII, as this was used in providing banking or other services.

164. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

165. Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

166. Defendants should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATIONS OF THE CONNECTICUT UNFAIR TRADE PRACTICES ACT
Conn. Gen. Stat. §§ 42-110a, *et seq.* ("CUTPA")

167. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

168. CUTPA states, "No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen Stat. § 42-110b.

169. Plaintiffs, Class members, and Defendants are "persons" under CUTPA. Conn. Gen Stat. § 42-110a.

170. The services that Defendants provide are "trade" and "commerce" pursuant to CUTPA. Conn. Gen Stat. § 42-110a.

171. Webster Bank made representations to Plaintiffs and Class members that their PII will remain private, as evidenced by, *inter alia*, its representations regarding privacy on its website. Webster Bank committed deceptive acts in violation of CUTPA by failing to inform Plaintiffs and Class members that Webster Bank would not adequately secure Plaintiffs' and Class members' PII by contracting with parties that did not have adequate safeguards in place to protect PII.

172. All Defendants engaged in unfair acts in violation of CUTPA by failing to implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class members' PII in a manner that complied with applicable laws, regulations, and industry standards. The failure to implement and maintain reasonable data security measures offends established public policy; is immoral, unethical, oppressive, unscrupulous; and substantially injurious to consumers.

173. Due to the Data Breach, Plaintiffs and Class members have lost property in the form of their PII. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding their customers' PII will force Plaintiffs and Class members to spend time or money to protect against identity theft. Plaintiffs and Class members

are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII without appropriate and reasonable safeguards to protect such information.

174. Plaintiffs and all other Class members were damaged by Defendants' violation of CUTPA because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased and imminent risk of identity theft—a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII was breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT VII
DECLARATORY JUDGMENT

175. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

176. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

177. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' Private Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their PII. Plaintiffs and Class members remain at imminent risk that further compromises of their Private Information will occur in the future.

178. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect Plaintiffs' and Class members' PII.

179. Defendants still possess Plaintiffs' and Class members' sensitive PII.

180. To Plaintiffs' knowledge, Defendants have not announced that they have remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

181. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach affecting Defendants. The risk of another such breach is real, immediate, and substantial.

182. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

183. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

184. Plaintiffs therefore seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. ordering that Defendants engage internal security personnel to conduct testing, including third-party security 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;

b. ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. ordering that Defendants purge, delete, and destroy in a reasonably secure manner any PII not necessary for provision of their services;

e. ordering that Defendants conduct regular database scanning and security checks; and

f. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive PII, including, but not limited to, the personally identifiable and financial information involved in the Data Breach.

PRAYER FOR RELIEF

Plaintiffs, individually, and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 24, 2023

Respectfully submitted,

/s/ Adam Pollock
Adam Pollock
POLLOCK COHEN LLP
111 Broadway, Suite 1804
New York, NY 10006
Tel: (212) 337-5361
adam@pollockcohen.com

Local Counsel for Plaintiffs Mark S. Holden and Richard Andisio

Ben Barnow*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: (312) 621-2000
b.barnow@barnowlaw.com

Charles E. Schaffer*
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
(215) 592-1500
cschaffer@lfsblaw.com

Interim Co-Lead Class Counsel

*admitted pro hac vice